

digit **FastTrack**

YOUR HANDY GUIDE TO EVERYDAY TECHNOLOGY



to **BACKING UP YOUR DIGITAL LIFE**

- Why backup is so easy today
- The basics of data backup
 - Save your social data
 - Preserve your PC
- Manage your Mac backup
 - Lookout for your Linux
- Backing up your smartphone (all OSes)
 - Save up your passwords
- Backing up miscellaneous data
- Recovery - for those who didn't backup





**www.
digit.in/forum**

Join the forum to
express your views
and resolve your
differences in a more
civilised way.

**digit.in
FORUM**

Post your queries
and get instant
answers to all
your technology
related questions



One of the most active online technology forums
not only in India but world-wide

**JOIN
NOW**

digit.in



Backing up your digital life

powered by

digit
YOUR TECHNOLOGY NAVIGATOR

CHAPTERS

Backing up your digital life

AUGUST 2014

05

PAGE

Introduction: why backup is so easy today

This chapter shows you why a Plan B is important for storing your data and an overview of the options out there

13

PAGE

The basics of data backup

Some basic measures to take before, during and after backing up your data

18

PAGE

Save your social data

You use a dozen social media accounts, but have you ever worried about losing your data or how to keep it safe? We tell you all you need to know.

32

PAGE

Preserve your PC

In the era of mobile computing, the PC still remains the most important creation tool. Here's how you can back it up.

CREDITS

The people behind this book

EDITORIAL Executive Editor

Robert Sovereign-Smith

Writers

Avinash Kothuri
Daniel Dmello
Ketsan C
Niranjan Iyengar
Paanini Navilekar
Ronak Gupta
Vaibhav Kaushal

Assistant Editor

Siddharth Parwatay

Contributing Copy-Editor

Infancia Cardozo

Manager Test Center

Jayesh Shinde

DESIGN

Sr. Creative Director

Jayan K Narayanan

Sr. Art Director

Anil VK

Associate Art Director

Anil T

Sr. Visualisers

Shigil Narayanan
Sristi Maurya

Visualiser

Baiju NV

49
PAGE

Manage your Mac backup

OS X has Time Machine, but there are other tools you can use to back up your Mac.

56
PAGE

Lookout for your Linux

Let's not forget Tux shall we? In this chapter we show you how to backup your linux system

64
PAGE

Backing up your smartphone

Phones are prone to theft and destruction. And at the same time they carry your most precious data. Backup now!

77
PAGE

Save up your passwords

Yes even passwords can be backed up. Go through this chapter and you'll never lose another password ever again. In fact you won't have to remember one in the first place.

84
PAGE

Backing up miscellaneous data

In our quest to back up our digital life, we often forget the little things – bookmarks, saved games, sticky notes, contacts, form data and registry entries. This chapter will show you how to never leave anything behind.

91
PAGE

Recovery - for those who didn't backup

This chapter tackles some of the questions regarding data recovery that may possibly be nagging you

© 9.9 Mediaworx Pvt. Ltd.

Published by 9.9 Mediaworx

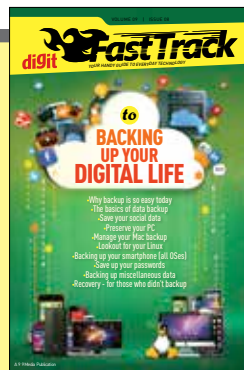
No part of this book may be reproduced, stored, or transmitted in any form or by any means without the prior written permission of the publisher.

August 2014

Free with Digit. If you have paid to buy this Fast Track from any source other than 9.9 Mediaworx Pvt. Ltd., please write to editor@thinkdigit.com with details

Custom publishing

If you want us to create a customised Fast Track for you in order to demystify technology for your community, employees or students contact editor@thinkdigit.com



COVER DESIGN: SHIGIL NARAYANAN

It's never too late to implement a backup strategy

As we continue to live our lives in the digital realm, the risk of losing it all becomes that much more real. Imagine the amount of data we have residing on our devices – be it PC, tablet or smartphone. Hundreds of personal documents, files, passwords, sticky notes, photos, and videos. Downloaded torrents can be acquired again but what if something were to happen to those precious memories that you've captured? Your child's first steps, that great birthday party you hosted when you turned 21; what if all of that is one day lost because you thought hard drive failure or phone theft is something that happens to other people and not you?

The thing with backups is that it never seems important until that very day when you need it. And now with cloud-backups becoming a reality, there really is no reason for you to not have a well thought out backup strategy in place. Most people see data backup as a difficult and geeky task that is beyond the reach of common users. The truth is that it's not at all difficult and you don't need to be a computer wizard to set up a basic data backup system in place.

In this FastTrack we'll do just that – help you figure out a backup system to suit your platform (Windows, Linux, and most of the common smartphone OSes etc.) and guide you through the entire process. Besides this we'll also show you how to get hold of copies of your online data. Yes, things in the cloud may be virtually indestructible but what if you lost access to say your Flickr account? Would that be a terrible disaster?

The FastTrack also highlights some of the little things that we often forget to backup and lastly for those who haven't setup a backup solution there's a chapter on recovery of lost data. Remember it's never too late. Happy reading. 

INTRODUCTION: WHY BACKUP IS SO EASY TODAY

This chapter shows you why a Plan B is important for storing your data and an overview of the options out there

Backups – What and why

In a much-used statement, it's safe to say that we live and revel in a digital age. We're dependent on technology like never before and with increasing dependence, we've built an increased need to manage our digital lives. From blog entries and code snippets to photo albums and music libraries, our data needs have gained priority making data backup increasingly relevant. While the concept of backing up data is not new, when applied to digital content it obtains an abstract sense that varies from the usual method of backing up important documents (creating photo copies).

However, in principle it's quite the same. Digital media is important, so you create backups. Simple. The reasons to back up your data are crystal clear. Our gadgets contain important and sometimes sensitive data that's extremely vulnerable to various attacks and modes of failure. In such an event, an efficient contingency strategy can be life saving, sometimes in the literal sense!

What is a backup and is it relevant to you?

If you own any sort of computing or digital device that hosts your data, a plan B is essential. Whether you're a student or a business owner, this is a critical need. Now that the term 'backup' has been thrown around aplenty let's get down to really understanding what the word means in this context. Put in the simplest of terms, taking a backup means generating a copy of any sort of data. The word 'copy' is of importance here and it must be clarified that the concepts of 'syncing' and 'backing up' are not synonymous with each other. A backup of any sort implies a data replication process. The data replicated may be stored in different media.

A data backup protects our content from a multitude of disasters. Our computers are hardly foolproof and are continually subject to some sort of hardware or software failure. Losing an important file due to a software crash may be disastrous if the file wasn't backed up. In case of a virus attack, most technicians will resort to a full system clean-up and again you may lose important data. Unlikely it may be, but our systems face the pervasive threat of natural disasters or power outages, which mete out damage to various machines. All these problems are avoidable with a disaster recovery plan. Who knows, somewhere down the line, you may thank Digit for saving your precious data should a voltage spike damage your laptop (God forbid!). A backup even ensures protection against the stupidest of occurrences such as accidental deletions. Long story short, you spend a major part of your life in the virtual space, generating large amounts of data. And if you don't, you will soon. The world is shifting to the digital space. Heck, even our very own Modi Sarkar is a proponent of e-Governance. In the wake of this revolution, it's very important to back up your data.

Cautionary tales

In a recently conducted study, 90 per cent of people don't back up their data. Another study by National Archives & Records Administration (NARA) found that 93 per cent of companies that lost their data centres for 10 days or more due to a disaster went bankrupt within a year. During Hurricane Sandy in the US, many companies based in lower Manhattan went offline and incurred avoidable data losses. Many companies don't seem to employ any backup methods, including downright simplistic online backups. It should be pointed out that most of these studies are carried out by data recovery companies and should be taken with a pinch of salt.



This could happen to you

Most data losses happen due to hardware failure with human error accounting for only about 10 per cent (the number varies with each study). Data recovery cost varies anywhere from Rs.500 to Rs.60,000 for a hard disk and upto Rs.2,000 per file for some files! A

done-to-death proverb is easily applicable in this context – It's better to be safe than sorry.

Traditional methods of backup

While the current generation has at its disposal efficient media for small scale backup, it wasn't very long ago when floppy disks were among the few options for creating backups of important files. You may remember having used them to save your school projects on. Physical storage media has come a long way since then and we now have sophisticated devices such as flash drives, pen drives and external hard disks that offer storage space considered colossal when compared to the minuscule storage space a floppy disk offered.

A large population of users sticks to the above mentioned methods of data backup, now being considered as the traditional way of doing it. They



Sending data to remote servers in a great strategy

have their advantages: they're simple to use, require absolutely minimal technical assistance and have the added benefit of local presence. Plus, they don't require an internet connection to set up backups. However, there are some major pitfalls of sticking with these traditional backup options, many of which are notably absent in cloud storage, a fad that will be discussed in the upcoming sections.

Why these devices are on their way out

Most of these storage mediums are easily susceptible to corruption and exposure. Magnetic tapes could be damaged and drives have multiple components that are prone to failure or damage due to common occurrences.



The six form factors HDD come in

Theft is the number one cause of data security breach in the US and your external hard disk or flash drive is easy game for an organised theft. In addition to theft, these backup mediums can easily be misplaced. Backup on the cloud addresses this issue by using high levels of encryption and physical security.

As mentioned before, despite the odds being small your hard drive may be damaged in a natural calamity. Backup of a backup is a concept that's gaining popularity nowadays. However, users of traditional storage media are limited by space and are generally unable to create multiple backups of important data.

Last, but not the least, traditional data backup options are on site. In case you're shifting your workplace or business, you'll have to manually shift all your backed up drives taking care to avoid damage.

While traditional data backup techniques are still common owing to their simplicity and cost effectiveness, storage and backup on the cloud is slowly turning into more than just a buzzword. Cloud storage offers a sophisticated and largely failproof backup plan, one that anyone remotely in need of backup options must explore.

Enter the Cloud

In the past few years or so, the term ‘cloud computing’ has begun to gain popularity. What ‘cloud’ refers to is simply the collection of hardware and software at the back end that allow you to access specific services. Cloud-based backups are just one of the many services, which are slowly picking up.

Most people are already using cloud storage in some form or the other to create duplicates of their important content. Some are using outdated methods to do this, say, by sending files to their own mail addresses, while others have moved on to newer methods



Data farms – the cloud doing its thing

being offered by cloud storage providers (CSP). In a nutshell, cloud storage is a way of storing files on servers (spread across the world at times) and these files can most often be accessed via some sort of network.

Syncing as value addition

Popular cloud storage providers such as Dropbox and Microsoft SkyDrive already offer data synchronisation to users. You may also be familiar with cloud storage when it comes to email, that’s usually stored in the mail client’s servers. Photos taken by cameras – be it on smartphones or point-and-shoots – can be automatically uploaded to cloud services such as Google Drive for Android devices, OneDrive for Windows Phone and iCloud for Apple. Contacts can be backed up to the cloud and are retrievable using a browser should you lose your contacts due to damage done to the phone. Similarly, desktop users can install one of the many software products provided by CSPs and synchronise their important folders with cloud. The size of common office files doesn’t usually exceed the free storage space provided by CSPs. Additionally with cloud services like Google Drive you can access many common office files (like Microsoft Office’s doc files) using browsers. Then there’s also the ability to save music in the cloud, but many services that allow public sharing have copyright protection in place for



such media. Cloud-based services offer a large number of options and plans when it comes to storing and backing up data. Synchronising is just one of the many attractive options that serve as a value addition to backup.

Not just for companies

With emerging technologies and cheaper options, cloud storage is becoming a more viable option – not just for companies but individuals as well. Individuals who wish to protect important files from being damaged by anything, from earthquakes to coffee spills. Cloud storage offers many advantages over the traditional methods of storage. They aren't vulnerable to accidental deletion, computer viruses or misplacement. As an added benefit, they're off site and using multiple services you can have more than one backup at multiple locations to lower the chances of data loss in case of a natural calamity, power outage or server crash.

The cloud is providing exciting opportunities and services to fulfill the need of every kind of user. As our lives become

more and more intertwined by technology and digital devices, backing up any kind of data becomes more of a need than a luxury. Cloud storage is not only an attractive option but an extremely robust and efficient one too.

As easy as 1, 2, 3

Data backup is often seen as a difficult computer-based task that the common user shies away from. The truth is that it's hardly difficult and you don't need to be a computer wizard to set up a basic data backup.

One quick look at the backup process is all that's needed to realise that saving files on the cloud needs nothing more than a user name and password. Most of the aversion to cloud-based storage probably stems from the fact

that users don't understand the meaning of "backing up on the cloud" and aren't used to the idea of a non-local medium of storage. Cloud storage is safe, easy and efficient.

Big players like Google, Microsoft, Amazon and Apple ensure that you're aware of their forays into cloud storage. If anything, the trend is encouraging. And with each of them competing to be the best, the winners are probably the users who are already associated with them. Search giant Google offers Google Drive, which can be installed on a PC or accessed via a web browser. Drive lets you save attachments received in your mailbox. Additionally, any important files can be backed up by manually dropping them in the installed Drive folder. Linux users, on the other hand, are forced to use web browsers to access their files. With small(er) players such as Dropbox entering the picture, users can access their data regardless of which operating system they're on. Backing up has become as easy as dragging and dropping. Apps on your phone allow you to back up and sync photos, videos, music, text files, etc with not more than a touch. Many services prompt you to save your files on the cloud and the only requirement is a valid account and granted permission.

Even computer-savvy individuals have probably experienced some form of data loss or the other over the years. And with data recovery prices being sky high, it's highly recommended that any user label their files (at least in their head) as important or not so important. Data backup is an extremely simple procedure – one that can save you lots of hassle and prevent burning a hole in your pocket.

Why create a data backup? Why not!

Sample this. You live in an arid place, which hasn't seen rain in a century. But, global warming has another idea and floods your place with a down-pour one evening. You lose your research data, that's been painstakingly compiled over three years. Well, that's what you get for not taking preventive measures and relying on the law of chance and probability. This Fast Track aims to educate you how and why, if you use a computer excessively for any official, creative, social or business related work, you must have a contingency strategy.

There are many reasons why people don't take backups. "Nothing will happen to my data" is one of the most common answers that people come up with when confronted about slacking in this area. "Nothing?" Are you sure? If the whole talk about natural disasters wrecking havoc on your

digital life doesn't convince you, and the fact that data theft is one of the fastest growing crimes doesn't bother you, how about something as innocent and widespread as a computer virus? No anti-virus setup is foolproof and your system is susceptible to a large number of viruses that data security companies have never even encountered. A detailed survey estimates that a staggering 40 per cent of households are affected by a computer virus and 26 million new strains of malware popped up in 2011 alone! A potentially lethal virus can easily eat up data and corrupt important files. So, while the odds of an earthquake swallowing up your system are relatively low, the probability of a virus affecting your data is quite high. Your data is anything but safe.

Expenses and complications are other reasons people cite for not having a Plan B in place. However, backing up data is hardly expensive, especially when you compare it with the benefits. It's a very cost effective service. Local storage media like external hard drives are available for less than Rs.4,000 and have the capacity to satisfy more than basic data storage needs. When it comes to cloud services, most are available at no cost for lesser (but still sufficient) storage space so if you want to simply create multiple backups of small files then it's a near-perfect option. Online backup services are a bit expensive when compared to the above discussed options, but the former offers high levels of automation, ease of use and can be tailored to suit your needs.

You don't need to be a rocket scientist to efficiently back up data. Using an external drive for backup is as easy as drag-and-drop and cloud-based services are coming up with increasingly simple user interfaces to lure and encourage common PC users to create backups. The UIs are direction driven and usually feature a simple instruction-led process. Contrary to perception, there's no scripting, code-writing or complex installation of third-party software. It's a light and easy procedure.

Then there are those who claim to be too busy to take backups. While it's true that using traditional methods of backup can be time consuming, modern backup services let you save your files in preset intervals and create an automatic backup without interrupting routine. Backing up data is not a process you need to call your IT In-Charge for anymore. It's now become a user-friendly procedure that can be seamlessly integrated into your system security plan. 

THE BASICS OF DATA BACKUP

Some basic measures to take before, during and after backing up your data

There are certain things we know we should be doing regularly: frequently exercising, regularly oiling our vehicles, updating our passbooks and backing up our data – but more often than not, for whatever reason, we refuse to do them. The last one on that list though, if taken for granted will ensure that you regret the decision of not having taken early precautions. Neglecting this task will hit you quick and hit you the hardest. We're talking about losing all your precious data just because you didn't bother to back it up, of course. If you've gotten so far as this chapter, we've probably already drilled the importance of taking backups into your head. But, if you aren't sold yet, picture this: the music collection that you've worked for years to put together, or your most cherished memories captured in pictures, or even the documents that are the absolute backbone of your entire business – all gone in a matter of seconds, and you'll never EVER see them again! A fire, a hurricane, a virus attack, a power surge or just plain wear and tear – whatever be the reason (the possibilities are endless), you may as well just kiss all your files goodbye right now. So yes, while taking precautions might be a dull affair, in this age when we spend a majority of our lives in the digital world, backing up data is an absolutely indispensable activity. With the advent of mobility and a wide

choice of devices, data backup has also become a field that has grown by leaps and bounds, and today a wide range of backup solutions in the form of software is available to the average user, which we'll encounter in later chapters. For now, let's focus on the absolute basic things to do to ensure that backups are done in an effective manner.

► Sort and prioritise

One of the major problems with backing up data is the insane amounts of data that an average user now possesses. It immediately raises the point that not all the data on your hard disk is equally important.

There are those files that are absolutely crucial to you, and then there are those that, even in case of a disaster, won't take much effort to re-attain. For example, it would be so much more painful – excruciating, in fact – to lose your private documents (photos, articles etc.), in comparison to losing that Miley Cyrus .mp3 file. So, the first thing that you should do is sort and prioritise your data. Give most importance to data that's personal, unique or



Have data backups traditionally as well as on the cloud

irreplaceable, and back them up without further ado. This is the content you want to protect no matter what – so limitations in terms of storage space or bandwidth (for cloud storage) shouldn't pose as barriers. This will also help you clean up old files that are no longer relevant to you, reducing the amount of data on disk.

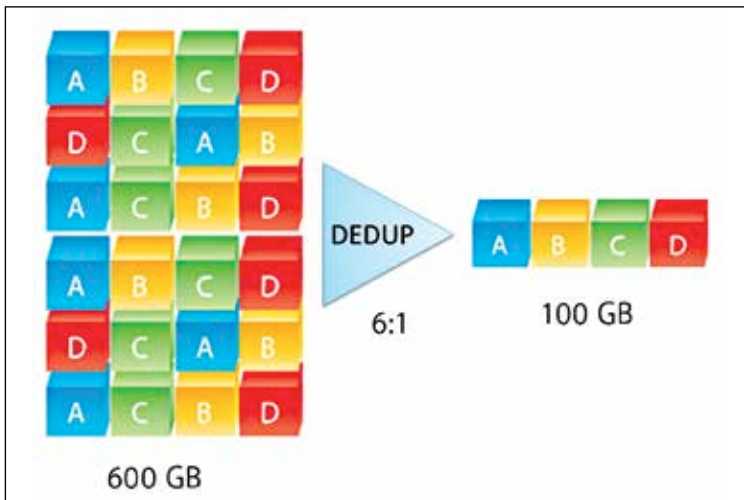
Once you do this, broadly classify your data into two primary categories: critical data that needs to be backed up regularly and data that doesn't change much over time. This would eliminate the redundant task of taking unnecessary backups.

► Remove duplicates

Also, having duplicates on the same drive isn't going to be of much help. But for the one-off accidental deletion, duplicates only serve to take up extra space on your hard disk and nothing else. Therefore, installing a deduplication software might help in removing redundant files.

► Compress

This brings us back to the major problem with backing up data – sheer size. Sometimes the hard disk you possess doesn't have enough capacity to hold all the data that you need to back up, and sometimes bandwidth might pose as a barrier for backing up huge amounts of data. That's where compression comes in. So wait, what is compression? Compression is basically just reducing the size of a particular file which can again be expanded back into its fully functional form. Now, it might seem quite mysterious how these bits and bytes of data that were cut down can regain their original state later. Well, the basic idea is fairly simple really. Most computer files are fairly redundant in the sense that they have the same information listed over



Deduplication frees up a lot of space

and over. What compression software does is it gets rid of this redundancy, lists a piece of information only once and refers back to it over and over again whenever it appears in the original program. To make it clearer, let's consider the statement "I think therefore I am". So if we assigned numbers to the words like this:

1. I
2. Think
3. Therefore
4. Am

Then our sentence would just be 12314, using only four words where one word which is redundant is deleted and upon being called refers to the piece of information that's already available (1, in this case) – thus making the sentence smaller.



Winrar is one of the more popular data compression softwares

There are two types of compression: 'lossy' and 'lossless'. Lossless compression is the type of compression that returns the entire original file upon expansion. Lossy compression cuts down on the unnecessary bits of information, thus despite being incomplete, the file will still be entirely functional.

Now that you have a fair idea of what compression is, you'd do well to know that one of the most important applications of data compression is in data storage, of course. The amount of data we produce is continuously expanding, and this coupled with the limitations on bandwidth clearly makes data compression the need of the hour.

So yeah, our advice – use popular compression tools such as WinRAR or 7-Zip to compress your files and save up on space.

► **Back up on physical devices and the cloud**

External hard drives or USBs are very susceptible to physical damage in case of accidents or disasters. Storing on the cloud, on the other hand, poses bandwidth limits and a potential security threat to your data. So just to be safe, make sure you have both, physical as well as cloud backups of your most important files.

► **Keep your computer clean**

We're talking about infections of course. Be extremely wary of email attachments and anything else you download off the internet. Regularly scan your computer and ensure that your files are all clean before proceeding to carry out your next backup. You don't want a virus corrupting the drive you've already backed up your data to, do you?

► **Protect sensitive data**

Make sure your sensitive data and its backups are protected. You can either password protect your documents or use the encryption tools built into your OS. Also, make sure you completely destroy any media that's become

dysfunctional before discarding it. There are more ways than you know of recovering your data.

► **Don't store your documents on the same drive as your OS**

This may sound like basic advice, but is a big no-no. Most software products install or save files in the My Documents folder of your primary drive (usually c:\), but this is the worst place to have them saved. Why? Sometimes, there are software failures or viruses, which would require you to reinstall the OS and thus format the entire drive. This would mean losing all the data on your drive, and is exactly why you should always have separate drives for your data and your operating system. You can just partition the drive using partition software and save your data in the new partition – beware though that doing this may violate the warranty conditions on your hard disk. Alternatively, you can just get an additional internal or external drive to store your data separately; which also helps you take the next measure.

► **Keep backing up!**

The best practice for effective backing up: regular backups. We know we've made this clear, but backing up your machine regularly can protect you from the unexpected. Files you'd want to back up from time to time might include data such as your recent documents, application data and, most importantly, system backups. Sure, you can always reinstall Windows (or any other OS) and your apps in case of failure, but switching to a recently created system backup (a.k.a a disaster recovery backup) will ensure that the transition is much smoother. You could just program your OS to automatically back up for you in scheduled time intervals.

► **Keep verifying your backup data**

You want to ensure that the backups you're taking are indeed being stored in a retrievable manner. Imagine spending all that time to back up data only to find out that it wasn't being done as you intended, or – to your absolute horror – that the files weren't really being stored at all! It might be time consuming, but verifying that your backed up data is indeed present and in its latest version is essential to ensure reliable backups.

There you go. We've covered the absolute basic things to do to ensure that your data is safe. These are generic measures that everyone must take. We'll be focusing on the more specific backup solutions available to you over the next few chapters. 

SAVE YOUR SOCIAL DATA

You use a dozen social media accounts, but have you ever worried about losing your data or how to keep it safe? We tell you all you need to know.

We use a variety of different digital tools to create and share content online. This social media data is being constantly updated, along with our needs and how we see ourselves using these tools. What may have been cool once is not cool anymore, and we tend to stop using a tool after a while, leaving an online presence behind, with what might potentially be sensitive information that is better off being erased from the internet altogether. Of course, some of this information has sentimental value, and a need arises to make a copy of this data before destroying it. Another personal reason you might have to back up your data is to get a historical perspective of the data you created, to see how your Internet behavior or writing habits have changed over the years.

Other people might manage social media tools and create content for professional reasons, and a need arises to maintain backups or digital records in case of emergencies where data can potentially be lost, or for legal reasons. For both these reasons, it is important to know how to backup,

export, archive or download the data that you create or manage online. We have provided you with instructions on how to do this, and have covered both backing up data using functionality present in the social media tools themselves, and backing up data by using third-party applications that connect to social media tools.

Back up from the original site:

We have presented nine popular social media applications below with details on how to back up your data directly from them, by using functionality that they provide within the application itself. Most of these are simple and straightforward techniques.

1. Facebook

Facebook allows you to download all of the personal information that you have uploaded to it since you created an account. This includes your personal profile information on the About Me page (your birthday, hometown,

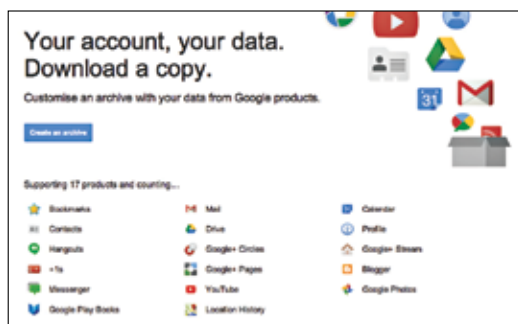


The backup might take a while to download depending on how much information you have uploaded to Facebook since you became a member.

education, job history, relationship status, family members, favourite quotes, languages, political and religious views), phone numbers, people you have added and removed as friends, followers, sent, received and pending friend requests, posts you created, posts shared on your wall by others, photos and videos you uploaded to your wall, photo metadata, chat history, event history, groups you belong to, apps, check-in history, poke history, notification preferences, privacy settings, hidden pages, ads you have clicked on, dates corresponding to your account being deactivated or reactivated, email IDs added and removed, and IP addresses that were recorded when you logged in or out of Facebook.

Downloading all this personal data from Facebook to store as a backup is quite easy. Go to any Facebook page at <https://www.facebook.com> > Click the down arrow in the top right corner of the menu bar > Click on 'Settings' > On the next page, under General Account Settings, click on 'Download a Copy' > On the next page, click on 'Start My Archive' > Re-enter your password > Click on 'Start my Archive' > Click on 'OK'.

Your archive will take some time to assemble. When it is ready, you will receive an email with a link to download your archive. Click on the link and then on 'Download Archive'. This email link will only be valid for a few days for security reasons, so keep an eye on your email. You will have to restart the download if the link does not work.



Google allows you to create a simultaneous archive from 17 online services in total, even if you aren't logged in to all of them.

Google products, which makes it easier for you to access and download data that you have uploaded to them. Since they all fall under one giant Google umbrella, the data is all in one place, so you can create downloadable archives for all of them at the same time, instead of wasting your time going to each site and creating individual ones.

To do this, go to www.google.com > Log in to your account > click on the profile icon in the top right corner of the web page > Click on 'Account' > Click on the 'Data tools' tab in the top menu > Click on 'Select data to download' > Click on 'Create an archive' > On the next page, un-tick a Google product for which you do not want to backup, or else leave them all ticked > Click on 'Create Archive'.

By default, your archive is generated in the form of a Zip file, but you can change this to a .tgz or a .tbz file. Depending on how much data you have, the archive may take hours or days to create. If the archive is larger than

2. Google

Do you have a Gmail account? How about Google Drive, Google+, YouTube, Hangouts, Calendar, Blogger and Photos? You do? Well the good thing about these is that they are all Google

2 GB, it will be split into multiple zip files. As before, you will be sent an email when your download is ready, with a link to the archive to download. Click the link and then click on Download, re-enter your password and then click on Download again. This link will only be valid for a week for security reasons, and the same archive can only be downloaded five times.

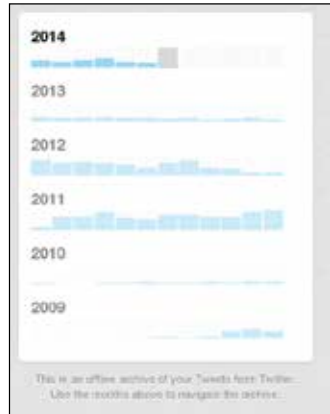
3. Twitter

Most people do not really see the point in backing up their tweets. Unlike information uploaded to Facebook or Twitter, tweets are generally neither valuable nor personal, and if they were sensitive it would be best to delete them. But you occasionally do feel like revisiting an old link or conversation, and scrolling through Twitter's API to find an ancient tweet is not a convenient option. This is where backups prove to be useful. Creating a backup for your information on Twitter is relatively straightforward.

Simply log into Twitter at <https://twitter.com> > Click on the gear icon in the top right corner of the menu > Click on 'Settings' > Scroll down the account page and click on 'Request your archive'. A message will be set to your registered email ID when your archive is ready to be downloaded. Click the link in this email. This will take you back to Twitter. Click on Download.

The archive will be in the form of a .zip file. Once unzipped, you will see a bunch of files and folders. The best interface to view your tweets is via file named 'index.html'. Double click to open and then click Open again if your browser throws up a warning message.

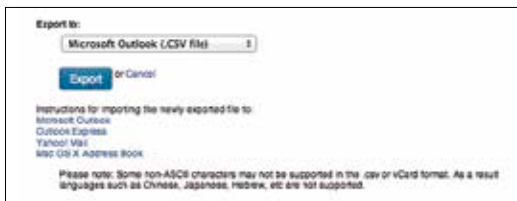
You also get to see the number of tweets you created each month, and view and favourite a specific tweet from your archive on Twitter. The downloaded archive has other uses. It contains a copy of your tweets in CSV format, which can be very useful for further analysis as it contains meta data for each tweet. It also contains a copy of your tweets history in JSON format, which is useful for developers. Browse the README.txt that come with your archive for more information.



The tweets for one month will be displayed on the page, and you can scroll between months using an easy to use navigator sidebar.

4. LinkedIn

The main reason anyone would want to back up their LinkedIn data is to make sure that they have a copy of all their contacts' information offline, though it would not hurt to also be able to download all their accumulated recommendations. We were not able to find any way to download our data



LinkedIn does not make it very easy for their users to backup all of their data in one go.

by going through the Account and Settings tab. We finally found ways to download our profile and contacts' information, but not information related to job searches, job appli-

cations, groups, message history, invitations, notifications, posts shared on the home page, recently viewed items, profile views and networks. And you will need to download your profile and contacts' information separately.

To download your profile information, click on Profile in the top menu bar > On your profile page, click on the down arrow next to Edit near your profile picture > Click on Export to PDF. What you get is a rather smart and professional looking PDF summarising everything on your profile page - your name, title, skills summary, experience, education and interests. You can also export someone else's profile as a PDF. Go to their profile page, click the down arrow next to 'Send a message', and click Export to PDF. These PDFs could also serve as handy quick reference CVs.

To download a list of your contacts' information, click on 'Connections' in the top menu > Click on the gear icon on the right > On the next page, under Advanced Settings, click on 'Export LinkedIn Connections' > Select the type of CSV or VCF file you would like > Click on 'Export' > Type in the Captcha text > Click on 'Continue'.

5. Imgur

Imgur does not offer a comprehensive solution to download images or GIFs that users upload to it. It also fails to offer a means to save for posterity the awesome comments and fake internet points that each post accumulates over time. It does however allow you to save albums, which is better than nothing. Log in to <http://imgur.com> > click on albums in the top right corner > Your

albums will be displayed in the new window. Click on the gear icon in the top right corner of an album window > Scroll down and click on 'Download album' > If your album is small, a ZIP file containing the images in that album gets saved immediately to the default download location on your computer.

As for the images and GIFs that are not in albums, the best way to download these is to manually save each one to your computer if you have just a handful. If there are many, the best way forward would be to create a new album, put the images in that new album and then save that new album to your computer.

Click on 'New album' near the top of the Albums page > in the next window, select Secret and save, since there is no reason to make this data public > In the next window, pick and choose the images that you would like to see in your new album



If your album is large, you will be notified by email when your album is ready for download, with a link to the download.

> Click Save. You can pick both single images that you have previously uploaded to Imgur, or images already present in other albums. Do note that only your images get saved, and not comments, points or other metadata attached to the images that are posted to the public gallery.

6. Reddit

When it comes to datasets, Reddit is synonymous with irony. The website prides itself on its users' ability to find and share datasets with each other. It also opens itself up to budding researchers and data geeks, letting anyone analyse its user data. But the situation is reversed when it comes to individual content stored on the site i.e. the posts, links or comments that users create or upload to Reddit. There is apparently no way for a user to download her or her personal data as a backup, which is a shame given the richness of the site's content. The best you can do is search through your user history of comments, submitted links and posts, posts you have liked, disliked, hidden and saved, and then save these pages or posts as HTML pages individually.



Another way to copy your data is to burn it as a series of RSS feeds.

Or burn it as a series of RSS feeds.

Log in to Reddit
 > Click on preferences in the top right corner
 > Click on the RSS feeds tab
 > Click on a specific service under private listings, private profiles, or inbox, for which you would like to generate a RSS feed

> Copy and paste the feed into whatever feed reader you use.

Note that this will not save data to your computer, but will allow you to access your historical Reddit data easily without having to browse through Reddit. One advantage with using RSS feeds for Reddit data is they tend to be more easily navigable compared to Reddit with all its nested distractions. Another advantage is that if you burn a feed early on as a user, you will still get to see your historical data in your feed reader. The downside is that you have no way to save your metadata, like Internet karma or gold earned.

7. Wordpress

You might decide to backup your blog in order to migrate it to a new blog location or simply to keep a copy of all your thoughts and comments safe. Data is more prone to deletion when a site has multiple admins. Wordpress lets users do this easily by letting them export their data as a XML file.

Log in to <https://wordpress.com> > Click on My Blogs in the top menu > Click on 'Dashboard' of the blog that you want to backup > In the sidebar of the next window, click on 'Tools' > Click on 'Export' > Click on 'Export' again if you don't want to pay for a Guided Transfer > Select the filter option > Click 'Download Export File'.



This will download your Wordpress posts, pages, comments, custom

If you choose to download only posts or only pages, you can further filter your download by category, author, date range or status.

fields, tags and categories. Images and other media that you have uploaded or linked to in a post should also get downloaded. If not, these will have to be manually downloaded to your computer, and uploaded again if you decide to export your backup to a new blog. Make sure your blog is marked as 'Public' and not 'Private' under Settings > Reading or your media may not download.

To export all the links from your blogroll, go to <http://dgit.in/ExportAllLinks> to generate a list (after changing the URL to reflect your blog name) and then save this list as HTML file via your browser.

8. Goodreads

If you are already a member of Goodreads, then you are aware that it is another social cataloguing website, like Pinterest, but one that deals with books instead of pictures. The site lets you rate and review books, begin discussions, create wishlists, build a network and share and see what your friends are reading. It can be linked up with other social media sites to import contacts, and with sites like Amazon for Kindle e-book support. This has led to the creation of a lot of good content around books and literature on the site. One would hope that some of this would be archive worthy.

Goodreads does allow users to export data of book they have read. Log in to Goodreads > Click on MyBooks in the top menu > Click on 'import/export' in the side bar > Click on 'export to a csv file' in the top right.

The CSV file contains the book ID, title, author, ISBN code, the user's rating, the average rating across Goodreads, publisher, binding, number of pages, year published, date added and information on the user's personal copy condition. Sadly, Goodreads does not yet allow users to export or download book reviews or discussions.

9. WhatsApp

As with any other chat platform, users may want to save conversations for future reference. WhatsApp lets you do this easily, by letting you export your chat history in the form of a text file attached to an email.

On Android phones, backup chats by going to WhatsApp > Menu Button > Settings > Chat Settings > Backup conversations. To export, tap and hold the conversation or group > Select 'Email conversation' > Choose whether to attach media.

On iPhones, you can backup your chats to iCloud. Go to WhatsApp Settings > 'Chat Settings' > 'Chat Backup' > 'Back Up Now'. You must be signed



WhatsApp is one of the most popular social media tools out there right now, and the amount of content being generated in the form of chat messages is mind-boggling.

into iCloud and have enough space on your phone for the backup. You can export individual conversations via email too. Open the conversation, type the contact or group name > scroll to the bottom and choose 'Email Conversation' > enter the email address > Hit 'Send'.

On Windows phones, in the main chat screen, tap the three dots at the bottom right corner > Tap 'Settings' > chat settings > backup. To export a chat, open the chat > tap the dots in the bottom right > tap info > tap the dots again > tap email chat history.

On a Blackberry, open the WhatsApp application menu > tap 'Settings' > 'Media Settings' > 'Backup conversations'. To export a chat, tap and hold a conversation > Tap 'Email conversation' > Tap 'Send'.

Back up from a third-party site:

We have presented seven third-party applications below. Most of these applications do not let you share or create content themselves, but sync with other popular social media tools, like the ones discussed previously, to archive your data in useful ways.

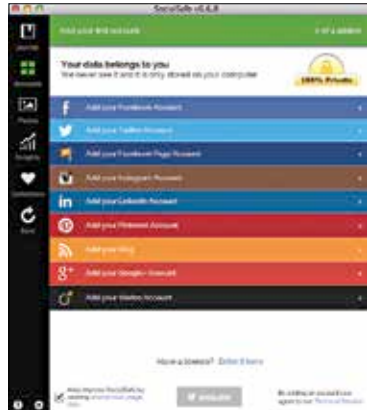
1. SocialSafe

SocialSafe was created to backup your social media data. It works by creating a library on your computer through which you can store and view all the data stored on your different social media accounts. It combines all this information into a combined timeline using a calendar, so users can see information shared on different social media accounts in context of a common timeline. It has a scheduling function that allows for the continuous downloading of new data from your accounts, and can generate analytics on data downloaded so far.

To get started, download the SocialSafe application from <http://www.socialsafe.net> > Launch the application > Select up to four social media accounts and link them to SocialSafe > Click on 'Sync'.

The four social media accounts that you decide to sync could take hours

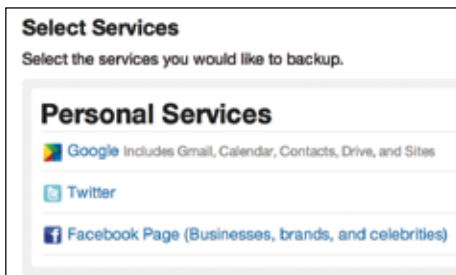
to do so depending on the amount of data you have on them. Once synced, you can view your data in the form of a journal. Clicking on any date will provide you with all of your social media activity on that day. You can also generate data for weeks, months and years. You can choose to view only your photos from any of the linked services. SocialSafe also allows you to export your data in CSV, PDF and ZIP format. You can do this for a specific entry by clicking on the boxed arrow at the top of the menu, or for an entire service by clicking on 'Accounts' and then clicking on the boxed arrow next to the service. It also offers a paid plan that lets you sync more than four accounts and use premium features for \$6.99 per year.



SocialSafe syncs up to four social media accounts from the following: Twitter, Facebook, Facebook Pages, Instagram, Pinterest, LinkedIn, Google+, Flickr, blogs and Viadeo.

2. Backupify

Backupify, like SocialSafe, backs up user data from multiple social media accounts, but it does this online with an option to back up locally on the user's computer once the online repository is complete. Once you register as a user, and sync up your accounts with the service, it backs them up to the cloud, encrypting them, and lets you download a copy to your computer as a backup. In this way, you have your data in two different locations. Backupify syncs up with Google, Facebook and Twitter.



Added security and professional support makes Backupify an ideal tool for business users.

To try the tool, go to <https://app.backupify.com/signup> > Enter your details to create a new account > Select the social media services that you want to sync with Backupify > These get added to your Backupify account.

The backup for Google archives Gmail, Contacts, Drive, Calendars, and Sites. Once setup, it collects email for the past 30 days, and keeps adding to and updating this with each backup. The backup for Twitter archives the tweet text, type and creation date. The backup for Facebook archives posts, albums, messages, friend lists and items in which the user has been tagged. Data from each service can be exported to users. Exports are emailed to users in a ZIP file and may take up to two days. Paid plans for midsize and large organisations are priced at \$99 and \$299 per month and come with greater storage, increased security, support and the ability to add more social media accounts.

3. Frostbox

Frostbox works like Backupify, backing up your social media data online, and offering you the ability to download a copy. It helps back up Facebook, Twitter, Gmail, LinkedIn, Foursquare, Flickr, Instagram, Tumblr and Evernote, making it the broadest social media backup service available. The information stored online is encrypted.



Frostbox also provides users with dashboards and lets you switch between backed up accounts online.

Go to <https://app.frostbox.com/main.php> > Click on 'Sign-up' > Enter your details and create a profile > Select a package > Select a service to sync it with Frostbox. Once synced, you can click into each social media service and download data from that service to your computer as a backup.

The Facebook backup archives albums, messages, friend lists and items the user has been tagged in, the one for Tumblr archives only original content, the one for Twitter archives tweets, retweets, followers, mentions and DMs, the one for LinkedIn archives profile information, connections, groups and companies followed. You can register for a free 7-day trial, but you will have to buy a plan after that for \$69.99 per year to keep your backup fresh.

4. Bulkr for Flickr

Flickr's latest upgrade has left users with 1 TB of free space. But while

users are busy uploading photos to the site, Flickr itself does not allow users to download photos en masse. You can only download a single photo at a time. This can be very frustrating when you have hundreds of albums and thousands of photos on Flickr, that you would like to copy to your computer. One way to get around this limitation is to use a third-party application like Bulkr.

Not only can you use Bulkr to back up your own photos to your computer, but also to download photos from any other user on Flickr. You can use it to download photos with a Creative Commons license. It even downloads photos from a search result and you can use the app to search through your photo stream. It also serves as a convenient interface to search for photos on Flickr. You can enter a tag or keyword, or enter a user photo stream URL or Flickr group URL to search through photos from a specific user or group. A Bulkr Pro version is available for purchase and allows you to view more photos per page and also allows for the capture of photo EXIF meta data.

The Bulkr application is available online as a free download. Go to <http://clipyourphotos.com/bulkr> and click on 'Install Now'. Once installed, authorise the app to connect to Flickr. Once linked, you can begin working with it. The 'You' tab allows you to backup and search through your photo stream or albums, and the Flickr tab allows you to search for specific photos on Flickr or its users or groups. It also allows for filtering by license, relevance, recency and date.

5. BackUp Jammy for Tumblr

Tumblr, like Pinterest, does not have a ready tool to allow its bloggers to download an archive of all their posts and comments. Perhaps it would be a good idea for Tumblr developers to begin working on one, given that Tumblr has experienced outages in the past, and was recently the focus of an attack from 4Chan users. Users might feel safer if they were able to archive their posts and comments. One such service that allows you to do this is BackUp Jammy.

Go to <http://dgit.in/TumblelogBackup> in the name of your Tumblr > Type in a post number as a starting point from where the tool can begin archiving > Select what data you would like to fetch > Click 'Go'. The application generates a HTML page consisting of all the text, links, quotes, photos, chats, videos and songs on your Tumblr. This HTML page can then be saved on your computer as a backup for future reference, in the same way as your Facebook data.



BackUp Jammy is a really simple basic web application that fetches your Tumblelog once you enter the name of your Tumblr.

If you prefer to store copies of actual photos and not entire HTML pages, then TumblRipper is a better option. This application, once downloaded and installed, scrapes all photos and videos from a Tumblr blog. You can download it at

<http://dgit.in/TumblRipper>. If it has already made one backup, it only downloads the most recently updated data, and downloads the highest resolution images available, so you do not get thumbnails. If you only want to download videos from Tumblr, you can do this with a dedicated browser extension like DownloadHelper available for Firefox at <http://dgit.in/DownloadHelperFirefox>.

6. Pin4Ever for Pinterest

The visual bookmark website that allows you to tag images that interest or inspire you does not in fact give you an option to download your data as a backup. We looked in the Account Settings with no luck. A search for terms like 'download' and 'archive' on the Pinterest Help Center did not yield any results either. Finally a quick search online led us to Pin4Ever, a browser extension that lets you create backups of your Pinterest data. The only catch is that you can only install it on a Firefox browser.



The extension also allows you to search through your Pinterest pins and move, copy and delete pins in bulk.

To install, go to <https://www.pin4ever.com> and click on Install Pin4Ever. The app will now run in your Firefox browser. To backup your data, open up Pin4Ever > go to the menu bar at the top of the page > click on Run backup > view a summary of all your Pinterest boards > make sure they are all ticked > Click on Backup selected Boards. Your data will get saved to a default download location that you can change by clicking on 'Settings' in the top menu.

A paid plan is available for \$49.99 per year. This offers additional power tools that allow users to find duplicate images and deleted pins, clean a home feed, view most popular pins, perform bulk image uploads, power follow or unfollow, backup follower data, restore user data from a backup, and offers advanced sorting options. This is an essential tool to use if you are a heavy Pinterest user or are using Pinterest for profession reasons.

7. Instaport for Instagram

Instagram is probably the World's most widely used mobile photo app, but strangely it doesn't come equipped with an export feature. This is something that users would find useful if they ever decided to delete their accounts but retain their data. Users could plug in their phones to their computers to back up their mobile photos, or transfer them wirelessly, but that defeats the purpose of Instagram altogether. Enter Instaport.



Instaport offers filters to create customised archives.

Once you authorise the app to link to Instagram via your desktop, it easily downloads photos in bulk from your Instagram account to your computer.

To make this happen, go to <http://instaport.me/> > Log in to authorise the app to link to Instagram > In the next window, choose your export options > Click 'Start Export' > Click to download your photos.

The photos may take some time to export given their number. For convenience, you can choose to only download a certain number of photos last taken, ones taken within a certain time frame, photos from others liked, photos with a specific tag, and videos, which turn out to be really useful options. The download will be saved to a ZIP file. 

PRESERVE YOUR PC

In the era of mobile computing, the PC still remains the most important creation tool. Here's how you can back it up.

We have come a long way in terms of backup techniques, from taking backups on CDs, DVDs to using software designed specifically for backup. Such specialised software bring with them various advantages like automation, synchronisation, encryption, compression, and various other benefits.

Types of backups

There are various types of backups that you can take. The choice for a backup type should depend on your requirement. Following are the types of backup that are there

Disk Image/clone

This makes an exact copy of the whole disk or a partition. You create a copy of the whole disk, sector by sector. Unless you chose to select otherwise, even the empty bits of data are copied. The clone can be copied to similar hardware and therefore even to install an OS in multiple computers with similar configuration.

File Backup

Here, you are simply copying a file to another location to keep as a backup. Earlier, you had to do this manually but now we have software that automate this process.

Synchronization

File Synchronisation may sound like File Backup at first but there are differences. In synchronisation, you have a mirror copy of the files selected by you at another location. Now what makes this different is that the mirrored copy is also a working copy and any changes made to it will reflect in the original file. Essentially, in synchronisation you have two 'sources' of files, unlike File Backup which has a 'Source' and a 'Destination'.

File Backup Terminology

Let us take a look at some backup-related jargon and see what they mean as a lot of backup software use these terms.

Full Backup

It means exactly what it says. It is a complete backup of the data selected by the user for backup. The files may be put in a single archive with compression and encryption, depending on the options selected by the user.

Differential Backup

In this method, only files that have changed since a last Full Backup are backed up in an archive alongside the Full Backup. Every subsequent differential backup copies the files that are different from the Full Backup even if they have been backed up in the previous differential backup.

Incremental Backup

Incremental backups only copy files that have been created or modified since the last full backup or incremental backup. While data redundancy is not as high as differential backups, it is still there as successive incremental backups will still contain files that have been backed up in the previous incremental backup but have been modified in some way. This system is faster than differential backup and even smaller in size.

Inbuilt Operating System backup tools

Windows XP

Not many will know this but Windows XP came with an inbuilt backup

tool which gave you the ability to backup the whole computer or selected files or drives. To access this backup utility, click Start and then click Run. Type 'ntbackup.exe' in the Open box and click ok. The Backup utility opens up in wizard mode.

Windows 7

Windows 7 came with a much more refined tool for backup than Windows XP. Using this tool you can backup specific files and folders and also create a system image if you want. For those who don't know what to back up you can let the tool chose for you. To access this backup utility, click the Start button, and then click Control Panel. In the Control Panel, click Backup and Restore. The backup and restore utility opens up. From here you can either create a backup, restore from a backup, create a system image or create a system repair disk.

Windows 8 & 8.1

Windows 8 & 8.1 has a nice new backup and recovery tool called File History. It allows for easy automated backup of your data and on a number of devices. To access this utility, go to Control Panel and click on System and Security. In this click on File History and the tool will open. Simply select the backup destination and click the "Turn on" button on the page to get started with the backup.

Backing up using 3rd party software

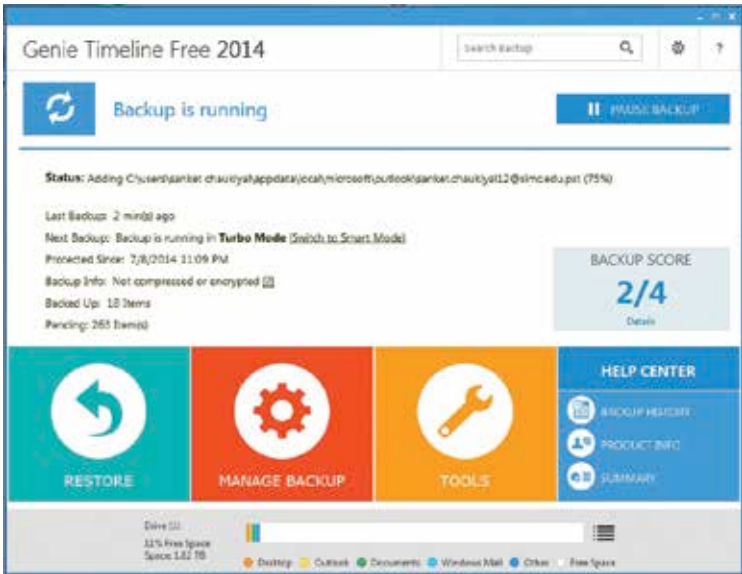
The best part is that a lot of good backup software is free. Backups can be of two types, offline backup where the backup medium is another physical storage medium and the second, online backup where the data is backed up to the cloud which can then be downloaded from anywhere.

Offline tools

Let us take a look at a few offline backup software that are currently making the rounds.

Genie Timeline

The first thing you are going to notice about Genie Timeline is its immense simplicity. You can simply set it and forget it, no need of continuous monitoring of the tool. The setup wizard is just a two step process to starting up your backup. First, you simply select the storage option where you want to keep the backup and next, you select what you want to backup. Genie Timeline makes it very simple for the novice user to select what they want to



Genie Timeline is one of the better options out there

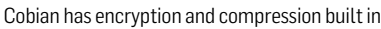
backup as, apart from letting the user choose which folders to backup, it has a feature called as Smart Selection which gives the option to backup email files, desktop files and folders, contents of the documents and downloads folder. In case you don't want to backup something, there is a 'No Backup Zone' folder created on the desktop in which you can put stuff that you want to exclude from backup. The restore options is again simple and gives you the option of selecting what you want to restore and to what location (original or new). Also, a great thing here is that you also get file versioning which allows you to restore files from a specific backup point. Genie Timeline also has an iPhone/iPad app in case you want to keep track of your backup.

The free version does not support encryption or compression and the minimum backup interval between each backup is eight hours. The advanced settings are also locked in the free edition.

For someone who is looking at simplicity of backup, Genie Timeline is the perfect offline backup tool.

Cobian Backup

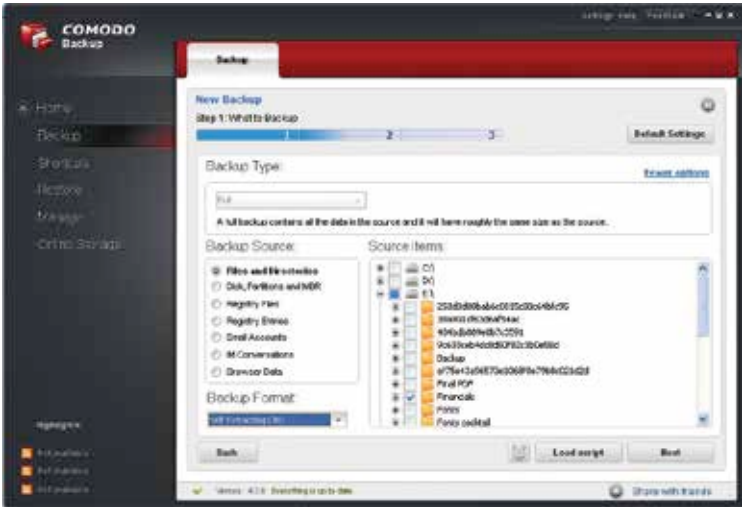
For those looking for a more advanced solution, Cobian Backup is another well known backup application which comes with a host of options like full,



zip compression features.
from an FTP server.

While Cobian has aced in the backup department, it surprisingly doesn't have an automatic restore tool. Unless you have selected the compression or encryption option, Cobian simply duplicates the files and directories in the backup location. You can head over to the backup location and copy the files that you want. In case if you have compressed or encrypted your backup, Cobian has provided the decompressor and decryption tools. Even though restoring data this way is as easy as copy-paste, it can become a nuisance when you have many incremental backup folders to go through.

Comodo seems to have got the balance right. It has a good mix of advanced features while still keeping the user interface simple enough for users. While you can choose what files you want to backup, it also gives you specific intelligent options like registry files, browser data, email accounts, etc. Backing up the system drive is as simple an operation as clicking the System Backup button on the main page which initiates an incremental sector-by-sector backup of your system. Comodo supports full, incremental and differential backup. Taking a backup on Comodo is a 3-step process, where, in the first step you select the backup source which can be files or directories, the entire disk or partitions, registry files, registry values, etc. You also select the backup type (full, differential or incremental) and format (depending on the backup source). In the second step, you can choose a backup destination from the Comodo Cloud (if you have a subscription),

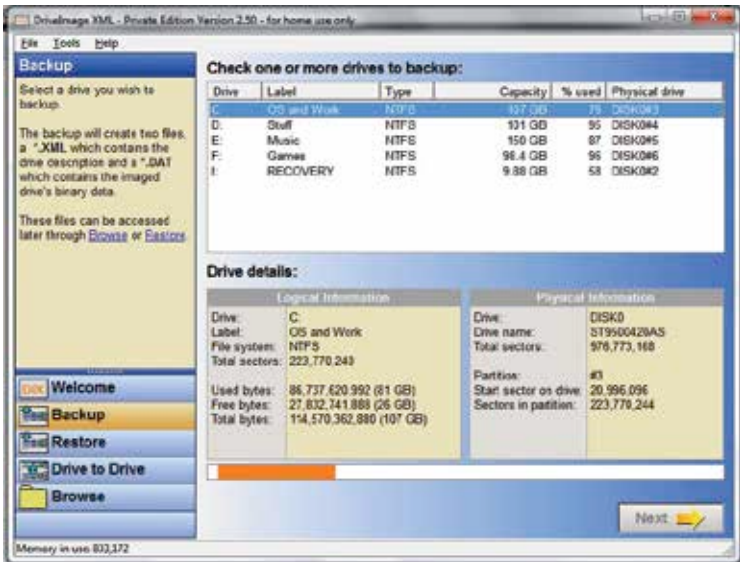


The first step of Comodo backup

location on your computer, CD/DVD, a network location, an FTP Server or also E-mail (depending on the backup source and format). If you want you can directly start the backup in the second step itself or schedule it for a later time, or you can go to the third step where you can modify the backup settings and then proceed with the backup. In the third step, before you backup, you can change the settings for the compression level, type of encryption, filters, Email Notification settings, and much more.

DriveImage XML

DriveImage XML, with its absolutely spartan interface, is one backup software that you will absolutely love or hate, depending on your requirement. It is a no nonsense backup tool which allows you to do only full backups of partition/s or the whole hard drive. Taking a backup is very simple. Simply go to the backup option and select the drive/s that you want to backup and click next. This will take you to the backup wizard through which you will select the backup location and the sparse options for backup settings. You get the option of setting compression level and also the option to copy the data sector by sector (this way even unused space will be copied) through raw mode. The backup creates two files, one dat file which contains the data and an XML file that contains the



DriveimageXML is quite different from the other tools.

description of the drive. DriveImage XML can lock up a volume to copy it or if the volume is being used then it can use Volume Shadow Service to get the last state of the drive.

Restoring is quite easy as well. If you want to restore specific files or directories, go to the Browse option and load the XML file for the backup. Then simply navigate in the file structure displayed and select what you want and extract it. And if you want to restore entire partitions or drives, click on Restore and select the drive where you want to restore the data to and select the XML file which contains the details of the backup being restored. Using the Drive to Drive option, you can copy one partition to another without creating an image first.

One good part about DriveXML is that it can also be run from the command prompt, which means you can create batch files for your backup purposes which you will only need to execute once to start the backup, all this without accessing the Graphical User Interface. If you want to schedule backups then you will have to use windows task scheduler. In conclusion DriveXML is very easy to use , can run scripts, and the backups are in a format that can be manipulated by other tools. On the down side there's no password protection and no option for file/directory level backup.

CrashPlan

CrashPlan is one of the widely used backup tools out there. One of its main USP is unlimited cloud storage option (free only for the first 30 days after which it is paid). However, offline backup is completely free. CrashPlan comes with many other unique feature which could make it your choice of backup tool from the wide variety that is available out there. Its systematic user interface makes using this software easy, which otherwise has many options that could confuse a novice user. Taking a backup is not an issue here as all options are neatly categorised. However, you are required to make an account with CrashPlan before you can use the software. The reason for this is that you get a unique code to identify your installation over the internet. We will see its purpose further ahead. The choice of backup destinations in the destinations tab is between your computer, your friends computer (more on this later), attached storage media or to the CrashPlan Central, its unlimited cloud storage option which is associated with your account. After you have selected the destination, you go to the Backup tab and select the files or directories that you want to backup. Then simply click Start Backup beside your choice of backup destination. You can even compact the archive post the backup from the Destinations tab which will



CrashPlan is quite a comprehensive tool

now show you the Compact button. CrashPlan is very versatile as it supports file versioning, scheduling, encryption, file exclusions, password protection for the application and the archive.

Restoring is as simple as going to the restore tab and selecting the file/directory you want restored and clicking restore. Here you have the option to select the version of backup that you want restored.

Now coming to one of the main USP of CrashPlan, backing up to your friend's computer. Basically, you can backup to other people's computer and they to yours if both have CrashPlan installed and have exchanged your 'backup codes'. These backup codes are unique to your account. Here again you can set limits and criteria for backup to your system and visa versa.

You can also maintain a backup between your other devices by installing CrashPlan with the same account, after which the other devices will start showing up in the 'Computers' list in the destination tab. With CrashPlan, the backup options are many. The unlimited cloud storage option which you get with a paid account is a nice addition. On the downside the inability to backup mapped drives in Windows is a bit of a downer.

EaseUS Todo Backup

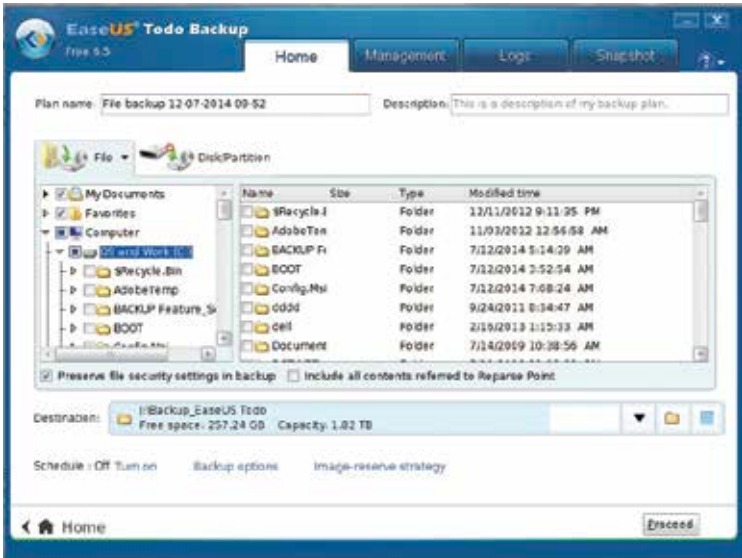
EaseUS Todo Backup packs powerful tools within its simple looking interface. It can backup files, folders and disks, partitions and can also take system backups. One added backup feature is that it can also backup Android devices. EaseUS Todo can also clone disks and partitions.

It is easy to initiate a backup in EaseUS Todo, just select the backup type and the files/directories/disks/partitions and then select the backup options, however, most of the advanced options are locked in the free version.

The recovery process is as simple as the backup process. Select the recovery type, select the backup file and then select whether you want to recover the whole backup or just specific files and folders. Here you also have an option to recover files from the backup by their file type.

Once you have selected the option, initiate the recovery. EaseUS Todo also supports Disk and Partition cloning. It is again a simple process and all you have to do from the Clone tab is, select the if you want to clone a disk or a partition and then select the specific disk/partition before you begin cloning. One good feature that EaseUS has here is that of doing a sector-by-sector cloning and also optimising it for SSD.

EaseUS todo has a feature called a Snapshot which records the state of your computer before system changes and if anything goes wrong, you can always



The EaseUS backup tool

roll back the operating system to these snapshot states. The PreOS feature of EaseUS Todo allows you to run the software before booting into windows in order to restore a system partition which has been corrupted. Here, you don't even require a disk or a flash drive.

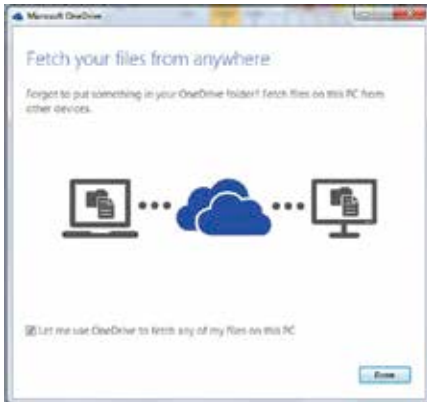
Backing up to the cloud

Till now we have backed up your data to offline drives, but there is always the possibility that because of some disaster you lose your data as well as your backup data and sometimes you need some data that is on your desktop but are halfway around the world? The solution to this dilemma is online storage, better known as cloud storage. There are a lot of companies out there offering cloud storage of which we have taken some of them which are better known and those that have something unique or a large storage space to offer.

Microsoft OneDrive

One of the largest players in the market, Microsoft's OneDrive offers 7GB of storage with the free account. While this may not seem much, it is good enough for storing all critical files and documents. OneDrive is actually more than just online storage, its an online office suite where you can create documents

on the cloud and edit and download them anywhere. OneDrive allows you to upload files through the web interface and it also has apps for the desktop and mobile. Once you download the desktop app, it will give you the option to syn-



Syncing files is easy

chronize all folders on your OneDrive account or specific folders. After installation, OneDrive create a OneDrive folder which contains all your synchronised documents and files. And if there are files or folders that you want to synchronise from your PC then all you have to do is place them into this folder and it will synchronise them. OneDrive can play your stream your video files online but surprisingly cannot stream

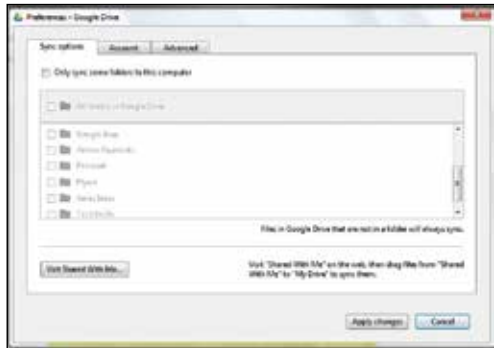
your mp3 files. It can also play a slideshow of the photos you have uploaded online. One nifty feature of OneDrive is that it allows you to access files on your system that are not in the OneDrive folder. It also allows you to access network locations if they are included in the PC's library or are mapped as network drives. Considering the less amount of space offered in the basic free account, OneDrive should be used more as a file synchronisation tool than a backup tool and should rather be used for important documents than for pure backup. OneDrive app is available for PC, Mac, Windows tablet, Android Devices, iOS, Windows Phone and Xbox.

Google Drive

Compared to Microsoft OneDrive, Google Drive offers a little more than double the space standing at 15GB for the basic free account. However, email attachments are also counted in this space. Google Drive is also an online office suite can can be used to create and edit documents online. Just like Microsoft's OneDrive, Google Drive also comes with a desktop based app that can be used to synchronise and backup content. Since, Google is offering a generous 15GB of storage, it can be used as a good backup source for your important files which could include photos, videos and audio. Like OneDrive, you will have to place your files and folders into the

Google Drive folder that's created in your explorer if you want to synchronise them. You can also upload files and folders directly through the web interface.

One area where Drive ups OneDrive is the ability to stream media files



Google Drive has come a long way

have uploaded any media, you can stream it online without the need to download it. Google Drive can stream both audio and video and like Microsoft OneDrive can display photographs online. Where it loses out to Microsoft OneDrive is remote PC access. Google Drive app is available for the PC, Android Devices and the iPhone and iPad.

Cubby

Cubby gives you 5GB of free cloud storage space in the basic free account (unto 25GB through referrals). It is a relatively new entrant in the cloud storage scene but has quickly gained a foothold in the industry mainly because of the innovative cloud service it offers. Cubby comes with a desktop based apps for PC and Mac and mobile apps for iOS and Android. When compared to Microsoft OneDrive and Google Drive, Cubby is more flexible because it allows you to designate any folder as a 'Cubby' (a synchronized



Cubby is worth trying out

folder). Which means that unlike OneDrive and Drive which require you to place the files in their respective folders for synchronisation, you don't need to change your organisation of files. Cubby offers versioning of the files synced to the cloud and can also create public links for files or an entire folder (Cubby). In case you have deleted something from one of your cubby folders and realise that you actually needed it then don't worry, cubby has the deleted version online which you can easily restore. Cubby can also stream your media files upto some extent.

In case you decide to go for the paid version, it offers an innovative feature worth mentioning even if it is a paid feature. Cubby offers something called as DirectSync where you completely bypass Cubby's cloud storage and directly synchronise unlimited size Cubby folders between devices.

Mega

Formed by Kim Dotcom after Megaupload's shutdown by US authorities, Mega veers heavily towards privacy. It offers you a massive 50GB of storage space with a 10GB monthly bandwidth limit. It comes with desktop apps for the PC and Mac and also apps for Android, iOS and Blackberry. Mega is very serious about security and has taken tough security measures for your data. All data stored online on Mega is heavily encrypted and is only decrypted once it is with you (on your device). Mega itself does

not have access to your encrypted data. Mega has an easy to use web interface. On your desktop, if you want to upload anything, simply place it in the Mega folder which shows up in the windows explorer. In case if you delete files, they will show up in the Rubbish Bin on the web interface from where you can restore them easily. You can also restore previous versions of the files by right clicking on them and downloading them onto your computer. Mega has custom sharing permission for data stored online, so you can define who gets to see what. Overall, if you are serious



Megaupload goes legit

about the security of your data on the cloud and are also looking for good storage space online the Mega is the one for you.

SurDoc

If your requirements are higher than 50GB then SurDoc is the cloud storage option for you. SurDoc comes with a massive 100GB for all your storage needs. Finally, a place where you can take a backup of your massive collection of photographs. The free account is almost at par with the paid accounts. It even has military-grade SSL security encryption. There is a catch however, after the end of a year; the only way you can renew your free account is by successfully referring a friend to SurDoc for which you will get 10GB per person. That means 10 people, which should not be so difficult. Plus, if you want more storage, you get 10GB for referring people to SurDoc and 10GB each for promoting SurDoc on social media sites. Not a bad deal.

The web interface is pretty simple to use, giving you the option to upload files, download them, share them, create new folders and even export some formats to pdf. When you delete a file from SurDoc, it goes into a recycle bin from where you can retrieve it unless you chose to delete it permanently. SurDoc has apps for the PC, Mac, Android and iOS devices. Using the desktop based app is pretty simple as well. Just select what you want you want to back up through the backup tab. You can even filter the type of files that you want to backup to the cloud. This is very helpful for those folders where you have mixed content but do not want to back up everything. The free account has a drawback though. There are restrictions on some file types, like for example, zip files cannot go beyond 5GB and executable and similar types of files cannot be more than 10MB in size. This limits your storage options of file types. However, there are no such restrictions on media or office files and so SurDoc can serve as an excellent option to backup all your expensive music collection and those family videos.

Data backup priority

Now the question remains, what are the important files that you should backup? Following is a list of important files that should be part of any backup list.

Personal or Business

Music, pictures, videos, documents, any custom template that you have downloaded/purchased, financial and health records.

System

Email files, internet bookmarks and shortcuts, paid software, drivers, game saves, paid fonts,

You can use any of the above offline or online solutions to easily backup the data. For the large files, offline storage is preferred while for the smaller files, online storage is a good option.

What not to backup

Do not backup your Windows or Program Files folder as this will be re-installed anyway if your computer crashes.

Are paid versions worth it?

While there is no doubt that the free versions of backup software have come a long way in terms of their functioning, there are still some great functions that are available in the paid versions of these tools. So if you have the money to spend then you can definitely go for paid versions of backup software. The following paid versions of the free software are definitely worth your money.

Offline Software

Genie Timeline: Considering that Genie Timeline has a very simple and easy-to-use interface. It is worth getting the full version for those who like a simple, easy to use backup interface as you can unlock more functionality.

CrashPlan: For those who are alright with an interface that gives you much more control, CrashPlan would be the recommended one. Along with the capability to store files offline, it also gives you cloud storage options with better encryption, unlimited file versioning, etc.

Cloud Based software

While you can always go for the sure-fire Google Drive and Microsoft OneDrive. The following are the ones that are positioned to offer you something unique.

Cubby: With subscription, get access to DirectSync which can be very useful if you want to maintain the synchronised data across devices and also the Device wipe ability to delete data off of stolen or lost devices.

Mega: If security is on your mind then you should subscribe to Mega which will give you massive, heavily encrypted storage.

Surdoc: Not much to say here except that SurDoc takes the cake with its unlimited storage plan.

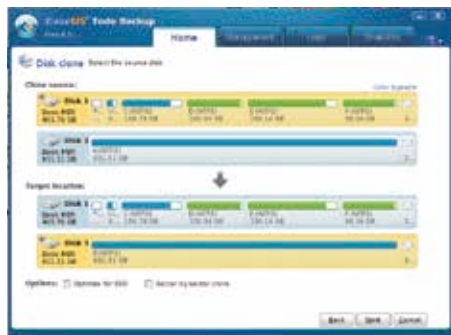
Backing up your PC

Any backup guide would be incomplete without showing the step by step procedure towards taking a complete backup or in this case making a cloned drive/partition. While there are many tools out there that will help you make a cloned drive/partition, the objective of this guide is to introduce you to a tool which helps you make a cloned drive/partition in the most simple way possible. While there are famous tools like Clonezilla used by people, they are however not for the first-timer. So, in order to stick to simplicity, we will use EaseUS Todo Backup software which helps you clone a partition or a complete drive with a simple to use GUI.

With EaseUS Todo Backup, you can clone your hard drive to a bigger one which eliminates the need to reinstall the operating system, applications, etc. Always note, the capacity of the destination should always be equal or larger than the source.

Tutorial: Cloning a drive/partition with EaseUS Todo Backup

1. First of all download the free version of EaseUS Todo backup software and install it.
2. Launch the software and then click Clone> Disk Clone
3. Select the Clone Source and Target Destination disks. You get two options, 'Optimise for SSD' which is useful if you are moving onto an SSD, and 'Sector by sector clone' which is useful to make an exact copy and will also map the blank bits from the source drive to the destination drive. Select the options you want and then click Next
4. Here you can preview the disk layout and make some adjustments. For example, if the destination drive is larger than the source drive and you haven't selected 'sector by sector clone' option then you can increase the size of the partition in the target location. Once you have made the changes you want, click Proceed to start the cloning process.
5. The final screen will show you the cloning progress. Yes you can clone entire hard drives



Here you can select the option to shutdown the computer after the process completes.

The process was as simple as that. Now that you have a cloned drive you can try out by booting up a computer with similar hardware with the cloned drive. With EaseUS Todo Backup, you can also clone individual partitions if you want instead of the whole drive. 

MANAGE YOUR MAC BACKUP

OS X has Time Machine, but there are other tools you can use to back up your Mac.

1. Time Machine

Time Machine comes free with your MacBook or iMac. It works on both normal external drives and on AirPort Time Capsule.

What does it back up?

Everything. It automatically backs up system and other files, applications, user accounts and preferences. After the first backup, it does this hourly and weekly for new files, depending on your preferred settings.

How does it work?

Plug in your external hard drive to your Mac > Click on the Time Machine icon in the menu > Open Time Machine preferences > Click ON > Select a



Time Machine is the basic backup application software used in Macs.

disk > Click Use Backup Disk. You will be notified when your backup is complete. If using your external drive as a backup for the first time, ensure that it is formatted or partitioned properly.

Leveraging its ability to backup both your files and system preferences, Time machine goes a step further and saves modified files separately. This allows you to restore your Mac and everything in it to the way it looked on a given day and time in the past, while retaining all the files from other times, in case you still need them. Time Machine allows you to encrypt your backup to make it more secure. Furthermore, it mostly works in the background while you work, so you do not have to set yourself reminders to backup your data. However, Time Machine can only backup to drives formatted in Mac OS Extended (Journaled) or HFS format. It does not recognise NTFS or FAT formats, which is what Windows compatible drives or flash drives use. You could reformat or partition your NTFS/FAT drive to enable it to backup your Mac's data.

Requirements

Mac OS X 10.5 Leopard or later.

Price

Free.

2. AirPort Time Capsule

The AirPort Time Capsule is a device that is built to work automatically with Time Machine, and works pretty much like any other external drive, with one exception – it is wireless.



AirPort Time Capsule holds up to 3 TB of data.

Like the two other Apple products from the same family - AirPort Express and AirPort Extreme, it also functions as a Wi-Fi router, offering dual bandwidth (2.4 GHz and 5 GHz) and 108.11ac. But while the other two devices are merely Wi-Fi routers, AirPort Time Capsule serves as both a router and a storage device. It comes with wired support if that is what you prefer using.

What does it back up?

It backs up the same data that any other drive does with Time Machine

- system and other files, applications, user accounts and preferences. It also saves multiple versions so you can pick which one to restore and use.

How does it work?

Your Wi-Fi network should detect AirPort Time Capsule automatically. Click on Time Machine preferences and follow the same instructions as you would for any other hard drive.

Click on the Time Machine icon in the menu > Open Time Machine preferences > Click ON > Select a disk > Click Use Backup Disk

AirPort Time Capsule backs up wirelessly and allows you to encrypt your data. And because it syncs via Time Machine, it does all of this automatically in the background, without you having to do anything. It detects when you are connected to the Internet and backs up your new files right away, without prompting you, and notifies you when your backup is complete. Like any other Mac compatible external drive, it only stores data in HFS format.

Requirements

Mac OS X 10.5 Leopard or later.

Price

₹19,790 for 2 TB and ₹25,780 for 3 TB.

3. Carbon Copy Cloner

Carbon Copy Cloner (CCC) works like Time Machine or Time Capsule, cloning your data to either an internal or external hard drive, and allowing you to work from there in the event of a hard drive crash.

What does it back up?

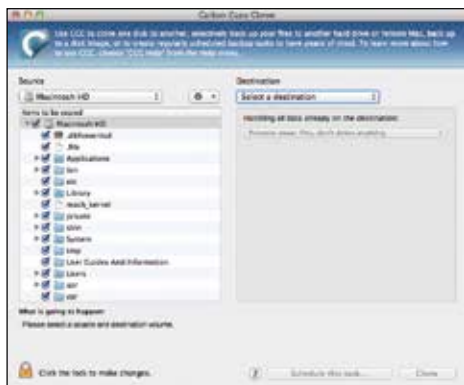
Everything on your computer.

How does it work?

CCC can be downloaded from www.bombich.com. To create a bootable backup of your OS X startup disk, plug in your external drive.

Click on CCC to launch > Choose the startup disk or file in the Source menu > Choose the new disk in the Destination menu > Click Clone.

If saving to your own drive, you can create a disk image for your backup. You can even instruct the application to begin backing up every time the external drive is plugged into your Mac.



CCC also allows you to backup to a remote Macintosh over a network.

CCC's restoration services act as a suitable alternative to Time Machine, and can save you if both your Mac and your Time Machine backup were to fail. Another advantage is that CCC also backs up data to non HFS-format drives. But keep in mind that this data does not include your recovery disk and would not be bootable.

CCC will not copy system files if you are creating a backup on your existing HD, to avoid system instability. For this reason, it is better to use an external hard drive to clone an entire disk. Also, not all external hard drives are bootable even after reformatting. Check online to see if your external hard drive is bootable via CCC.

Requirements

The newest version of CCC 3.5.5 requires Mac OS X 10.6 Snow Leopard or later.

Price

The trial version is free and valid for one month. You can purchase a permanent license for ₹2516.19.

4. SuperDuper!

SuperDuper! is a third party application like Carbon Copy Cloner, that allows you to create data backups on a hard drive. Like CCC, it allows you to clone your Mac's disk on an external drive so you can quickly reboot your system in the event of a system or local hard drive failure. In this way, you can keep working out of your external drive instead of waiting for your local hard drive to be repaired.

What does it back up?

Everything. SuperDuper! can create a clone of your hard drive or backup only specific files that you want.

How does it work?

You can download SuperDuper from <http://dgit.in/SuperDuperDownload>. Unlike Carbon Copy Cloner, this version is permanent and does not expire. However, a more advanced version that provides you with additional features like scheduling and smart updates, which are considered basic features



SuperDuper! Is now compatible with Mavericks.

on backup applications like Time Machine, can be purchased separately.

Launch SuperDuper!

- > Select your local Hard drive in the 'Copy' menu
- > Select the destination drive in the 'to' menu
- > Click 'Copy Now'.

In addition to creating bootable backups, SuperDuper! can also serve to test multiple versions of an operating system, and to quickly defragment a hard drive. Instructions for this in the form of white papers can be found at the same link above. You can also run shell scripts before and after copying, in the 'Advanced' tab. There are no obvious disadvantages but as before, you need to check your external hard drive to make sure that it can be used as a bootable drive.

Requirements

The latest SuperDuper version 2.7.2 is compatible with OS X 10.6 Snow Leopard and later.

Price

The basic version is free. The advanced version is ₹1833.38.

5. iCloud

So far we have discussed applications that create bootable backups of your data. However, it is good to have some data in the cloud for quick and easy access to everyday work projects that change by the



iCloud is the default online storage application from Apple.

minute and only get backed up online in real time. This is where iCloud comes in. It backs up your data to an online server instead of an external hard drive.

What does it back up?

Mail and Notes, Contacts, Calendars, Bookmarks, Photostream, Documents and Data.

How does it work?

iCloud comes installed on all Apple devices. You can set it up by clicking on System Preferences in the Apple menu. Log in using your Apple ID, or create one. In the next window you can choose what services you want to sync with iCloud. You should then be able to access this data anywhere or download it onto a new device.

iCloud works on both Apple and non-Apple devices, so once you upload data to iCloud, you can view and download it on anywhere. Also, once your data is on iCloud you can choose to share it with whomever you want easily since iCloud pushes your data to all your devices.

iCloud's main disadvantage might just be its convenience. You may become over dependent on it, and a hacker or security flaw might lead to you losing all your data. It is best to back up your data on an external hard drive as well. Another disadvantage is that it does not store disk recovery data. This means it cannot restore your system as it was in the past, or enable you to continue working uninterrupted in the event of a system failure. Our recommendation would be to use it as a backup only for information you intend to share.

Requirements

Mac OS X Lion or later.

Price

Free up to 5 GB. ₹1100 per year for 10 GB, ₹2200 per year for 20 GB, and ₹5500 per year for 50 GB.

6. Backblaze

While cloud based storage services like iCloud, Dropbox and Google Drive enable you to maintain a copy of the files you are working on, there is always a chance however slim, that your data might be compromised. For this reason,

it is better to also maintain an online storage account as a last resort for your files, especially for business purposes. This is what Backblaze is for.

What does it back up?

All data types, including ISO, DMG and EXE files.



Backblaze uses native code and not Java, which the company claims is a security risk.

How does it work?

Create a username and password and then download the Backblaze application from <http://dgit.in/BackblazeDownload> and install it on your Mac. Launch and select hard drives to back up. It can work with an unlimited number of drives. It also keeps files that you delete from your computer for 30 more days. Data is encrypted and they also have a mobile app that lets you download files to your iPhone or iPad.

Backblaze detects when you are online and automatically backs up your drives. This includes external drives that are plugged into your Mac. It allows for unlimited storage, can take unlimited file sizes and also stores multiple versions of files for up to 30 days.

Backblaze does not clone your Mac completely. It does not copy system files, application information, temporary Internet files or podcasts. Also, business users or professionals who would like their cloud storage application to retain older versions of files should look at other options, like Arq Online Backup, available at <http://www.baystacksoftware.com/arq/>

Requirements

Mac OS X 10.5 Leopard or later.

Price

\$5 per month for personal users and \$50 per year per computer for business users. 

LOOKOUT FOR YOUR LINUX

Let's not forget Tux shall we? In this chapter we show you how to backup your linux system

You don't need us to tell you how important backups are - you probably (and should) know that already. In an age where we're living such a great percentage of our lives digitally - through our digital photos, digital music library and digital documents, it's imperative that you have a way of recovering your data should something happen to it. In spite of it, taking the time to set up a foolproof and automated backup system is something we'd rather put off until disaster strikes - when it's too late to do anything.

Configuring backups doesn't have to be an exercise in tech wizardry, and most backup tools, even on Linux, are of the simple set-it and forget-it type. Meaning, you configure the files you want backed up, the backup location and the backup frequency, and let the program take care of the rest. The backup utility will run in the background silently, without your intervention, and if set-up properly, restoring data from your backups should be a breeze. Having said that, you should practice restoring data from your backups at least once, as backups are next to useless if you don't have a way to safely and quickly restore your data and resume work.

How Do I Backup My Linux PC?

Linux's power is obviously in its command line, with tools like cron, rsync and tar providing the building blocks for a robust backup system. Cron is a system daemon that can be used to schedule any tasks to run automatically, rsync is a file-copying tool that speeds up file transfers by only copying parts of files that have been modified, and tar is tool (similar to WinZip) that is used to compress files into archives. While you can certainly get the job done by playing around with these command line tools, there are plenty of GUI options available that wrap around these tools with an easy point-and-click interface, sparing you from having to use the Command Line.

To demonstrate how to use such a tool, we've picked an example called LuckyBackup (more on this program later) to walk you through the process of setting up your backups and restoring files in the event of data loss.

1. Installation

LuckyBackup can be found in the repositories of Ubuntu, Fedora, Debian, Arch, OpenSUSE, Redhat, CentOS and even Windows. Ubuntu and Debian users can run the command

- `sudo apt-get install luckybackup`

to install it, while those using the yum package management tool (such as Fedora or Redhat) can use the command

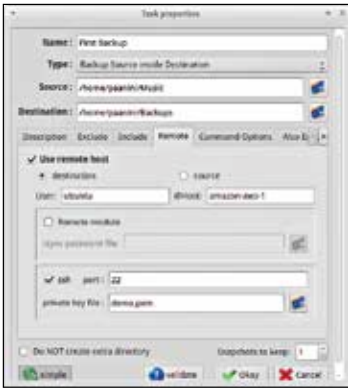
- `sudo yum install luckybackup.`

Needless to say, you'll need sudo (administrator) access to use any of these commands. Once it's installed, you can start the program from your distro's Application Menu > System.

2. Configuring your first backup

LuckyBackup lets you create separate profiles, so you can separate the backup up of say, your photos from your important documents or system files. Individual profiles can be run on different schedules or can be backed up to different destination folders.

To start, you'll need to create your first profile by clicking on the 'Add' button in the right column.



While setting up, you can choose to backup to/from a remote server.

You can choose to include or ignore certain files, preserve permissions of the files, set how hard-links will be treated and even have custom commands run before/after the execution of your backup. The 'Validate' button shows you the exact rsync command that will be executed when you run this profile, so you know exactly what's happening under the hood.

3. Performing a Dry Run

One unique feature of LuckyBackup is that you can have it do a dry run for you by simulating the backup process, alerting you of any failures, file deletions or size constraints that you may run into. Additionally, if your remote server is improperly configured, you'll receive an error so you can rectify the settings. This is just a precautionary measure - no files are modified/created during the process.

4. Scheduling Backups

It's not easy having to remember to backup your system every day or every week, and luckily, we don't have to. Luckybackup has a built in feature

Give your profile a name, choose the folder you want to backup, the destination directory, and you're good to go. You can choose the number of snapshots to keep, but be aware that increasing this number will consume more space on the destination drive.

If you want more advanced control over your backups, you can click on the Advanced button, which brings up a new menu. Here you can configure a remote server (either as the source or the destination) by supplying the hostname,



The Dry Option is handy since it lets you simulate the backup prior to running it

where you can select the frequency of a backup on a per-profile basis. This allows you to back up different kinds of data at different times. Choosing a frequency is simple enough, just use the drop down menus to select how often you'd like LukcyBackup to run, and it'll simply run the command in the background. Once you're done, click on the Cron IT! button to apply your changes. As you've guessed, LuckyBackup uses the cron daemon to schedule its tasks.

5. Restoring from a backup

Backing up is only one part of the game, the other half, being able to restore your data correctly and quickly, is just as important. After all, what good does a backup do if you can't restore it correctly? LuckyBackup has the restore feature built right in, and the process is very similar to the backup operation. Just choose the source (of the backed up files) and the destination (where the files should be restored to) and LuckyBackup will do the rest.

What programs can I use?

Linux has a wealth of backup programs available, and your distro probably came bundled with one. Whether you're looking for enterprise-grade backups with redundancy and encryption, or just a simple backup of your personal files to an external drive, this list has you



Scheduling is built right in, with fine-grained control over the frequency.



Scheduling is handled by Cron, so don't forget to press the Cron IT! button when you're done.

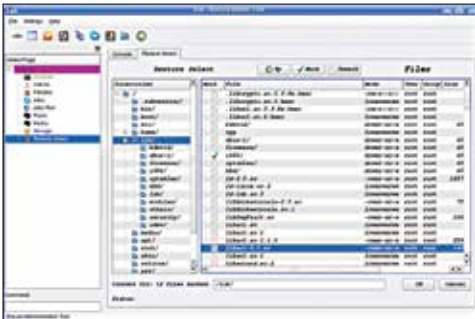


Restoring is handled within the app, with options similar to the backup ones.

covered. While there are of course a lot many options available, we've tried to pick a few that we think stand out in their segment. All the programs listed here are available in the default repositories of Ubuntu, Debian, Fedora, Redhat and OpenSUSE, unless stated otherwise.

1. Deja Dup

Deja-Dup is one of the most well-known of Linux backup and restore tools, as it is freely packaged with distributions such as Ubuntu and Fedora. It features a simple GUI interface that lets you choose which files you want backed up, the backup location (including local drives, networked drives, Amazon S3 buckets or Rackspace servers) and the frequency of the backup. You can optionally choose to encrypt your backups using a passphrase, and the program uses the Duplicity deduplication algorithm to save on space, as only changes made to files since the previous backup will be stored. You can instruct it to delete backups older than a certain age, or if you start to run out of space on your drive.



Bacula provides a highly robust, enterprise-grade backup system.

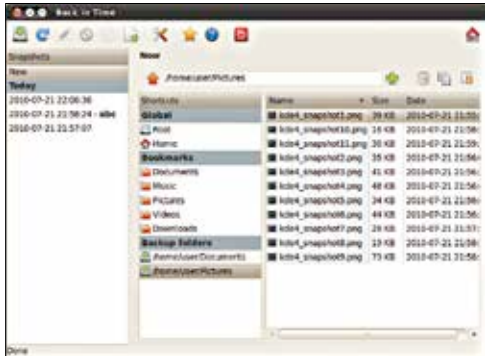
2. Bacula

Probably the only professional, enterprise-ready backup solution on Linux is Bacula, that sports a sophisticated client-server approach to backups. You can use Bacula's own GUI frontend or a third-party one like Amanda to configure your backups. The architec-

ture of Bacula consists of 3 main parts - the file daemon, that is in charge of collecting all the files to be backed up, the storage daemon that handles the storage location (which could be local or remote) and a director that maintains the configuration and scheduling operations. the configuration is stored in a PostgreSQL database, and all your data is encrypted before being sent over the network using the military-grade AES-256 bit encryption. While it may have a learning curve relative to simpler solutions, if you truly want a high-quality and cross platform backup solution, Bacula is your best bet.

3. Back In Time

Inspired by Mac OS X's Time Vault feature, Back in Time using the powerful differential file-copy tool rsync to create incremental backups on a schedule. Rsync uses sophisticated algorithms to generate diffs between two sets of files, only backing up those sections of files that have



Back In Time uses a snapshot based archiving system, backup only those files which have changes

been changed. Thus, this tool created snapshots of directories by comparing each file to its previous 'version'. Configuration options are quite limited, you can only choose the files to be backed up, the location in which to store the snapshots and the frequency of backups.

4. LuckyBackup

Written in Java, LuckyBackup is cross platform (works across Windows and Linux) and provides a nice middle ground between the minimalistic approach of Deja-Dup and a full-blown backup solution like Bacula. It sports a nifty 'Simulation' feature which can be used as a dry-run before actually making changes. You can use the Sync feature to keep any two directories in sync (either on the same drive, or on a remote location) similar to Dropbox, and it uses Rsync to create snapshots of your data to keep the backup size low. Additionally you can create separate profiles for backing up different kinds of data - you may wish to backup your photos to one place and your documents to another, for example.

5. Crashplan

Crashplan is a familiar name to those who're diligent about backing up their personal data, and with good reason. It's truly cross-platform, appearing on mobiles, tablets, and Windows, Linux and Mac computers. Onsite and offsite backups are completely free, and with a subscription you can get unlimited backups on Crashplan's servers. These backups are encrypted using a 448 bit AES algorithm to which you alone own the key, and before

being uploaded, and the connection is secured using TLS. Backups are continuous - i.e. your files are backed up by the minute. In the event of a catastrophe, Crashplan will even courier you a hard drive containing all of your data. Subscriptions start at \$4/month if you sign-up for a four-year plan. Business users can also avail of administrator functions by managing backups across multiple devices.



Crashplan is a fantastic option for those looking for a truly cross-platform, secure and automated backup solution

Crashplan isn't available in the default repositories of popular distros, so to install it, you'll need to download the installer from their website at <http://dgit.in/CrashPlanInstall>. It's a simple process that involves downloading an archive and then running a script, and they have step-by-step instructions on their site.

Where do I store my backups?

We're glad you asked. It's important that you give careful thought to where you're going to store your backups, for if the physical medium (or cloud provider) were to fail, it would result in massive data loss.

All backups must have an offline and an online copy for redundancy, so should your cloud storage provider go down (or face data loss due to syncing issues), you have a physical, offline copy handy. A NAS drive (Network Attached Storage), network location or even a dedicated Hard Disk will work well for a physical backup. For your cloud provider, we suggest you take a look at one of these:

1. **Dropbox** is by far the most popular file syncing tool, and while it is NOT a backup tool, it can work great as a secondary location to store your archives. The Dropbox client for Linux (available either as an Ubuntu package or a Python application) works well, monitoring your Dropbox folder for any changes, and syncing these changes to the cloud. While

- you only get 2GB of free storage, you can increase that using referrals, plus the Dropbox apps for Android and iOS are excellent.
2. **Insync** is a program that syncs with Google Drive (since Google hasn't provided an official Google Drive app), and in many ways exceeds the Drive app. It allows you to sync files from all over your hard drive to Google Drive, can automatically convert files to Office-friendly formats, and notifies you whenever someone makes a change to a shared document. Insync has a 15-day free trial, following which you'll need to purchase a license for a one-time fee of \$15. Well worth it if you're heavily invested in Google's ecosystem. (Additionally, Google Drive storage is the cheapest storage available at \$2/month for 100GB of storage)
 3. **Amazon S3** is the powerful web backend that powers several cloud providers and web hosts (including Dropbox, Netflix, and Instagram) and is possibly the most reliable cloud storage you can use. The first 5GB are free, following which you'll be charged as little as \$0.15/month for every additional GB. You only pay for what you use, so you don't need to buy into an expensive plan where you cough up several dollars for storage you're not even using. The downside is that uploading data to S3 is slightly tricky. Several third-party tools exist to ease the process, the most popular being S3cmd (<http://dgit.in/S3cmdLinux>). Available on Windows, Mac and of course, Linux. S3cmd lets you upload, retrieve and manage your data in S3, and also supports multi-part uploading (for large files) and encryption (for sensitive data).
 4. **Amazon Glacier** is a service that's tailored for long-term data storage, i.e. files that you won't need to access on a regular basis. With rates starting as low as \$0.01/GB per month, it's easily the cheapest option available, and with Amazon behind it, you can be assured of reliability. The catch, though, is that you can't use it for data that you need frequently, for Amazon charges you for data retrieval (beyond a certain limit). Besides, it can take up to 2 hours to retrieve data already in your archive, so if you need data to be restored immediately, you should probably use one of the other services. You can use the Simple Amazon Glacier Uploader (SAGU) to upload files to your account, available on Windows, Mac and Linux (<http://dgit.in/GlacierUpload>) 

BACKING UP YOUR SMARTPHONE

Phones are prone to theft and destruction. And at the same time they carry your most precious data. Backup now!

What's the first thing you do when you wake up in the morning? Odds are, you check your phone before you even brush your teeth. Likewise, what's the last thing you do before going to bed? Smartphones have embedded themselves so firmly in our lives, that they're literally by our side - whether we're awake or asleep. Being a hub of communication, information, entertainment and more, smartphones end up containing vast amounts of important data - from crucial ones like your contacts, email and photos, to more light hearted ones like saved game data and app preferences. What if something were to happen to this data? Your phone could get lost or stolen, it could suffer physical damage or it could be the victim of a malware attack - all of which would result in you losing your data for good, with almost no way of recovering the lost information.

In spite of containing such valuable and sensitive data, few users give thought to backing up their data, and fewer still do it in a comprehensive way. A survey by security company Avast revealed that less than half of smartphone users regularly backup their phones, yet more than 80% are concerned about losing precious data. Given the high stakes, it's pragmatic to have a robust backup system set-up on your smartphone, one that has your data protected in the event of any eventuality. This chapter has you covered - we'll show you multiple ways of backup up your Android, iOS, Windows or Blackberry smartphone.

I. Android

Android is easily the most widely used smartphone Operating System in the world - according to most reports, about 70% - 80% of the world's smartphones run some version of Android. Luckily, Android's open nature enables a whole host of options with regards to backing up your data - from simply using apps to backup your SMS and photos, to using the recovery mode to create a full system backup of everything on your smartphone. The latter is more complicated and requires an unlocked bootloader, but we'll walk you through the process in a later section. While the title of the chapter may say smartphone, these backup systems are equally applicable to tablets running Android.

1. Google Backup

Nearly all Android phones come with a full suite of Google apps installed, including Google Play Services - which enables, among other things, access to the Google Play Store. When you sign in to your Gmail account on your phone, Google automatically backs up a few important settings and data, and you can choose to restore data from this backup should you sign in to another Android device (or if you perform a factory reset of your device). To make sure this is enabled, go to Settings > Backup and Reset and check the box for "Backup my data". Some of the things that Google backs up to your Gmail account are:

a. Contacts

Contacts are probably the most important data on one's phone, so it's important that you turn on Google Contact Sync (Head over to Settings > Accounts > Google and check the box next to Contacts). When you enable contact sync, Google syncs all of your contact information into the cloud, where

it's available in the 'Contacts' section of Gmail. Any existing contacts in Gmail will be integrated into your phone, and any new contacts you add to your phone will be synced over to Gmail. This is by far the easiest way to keep your contacts backed up - it even lets you seamlessly transfer contacts between different devices (Android or otherwise). You can even view and edit your contacts in the cloud - on Gmail's web interface, click on the arrow next to 'Gmail' in the top right corner to reveal a drop-down menu. Choose 'Contacts' from the drop-down, and you'll find all of your contacts listed here. You can create and edit groups, edit information and manage duplicate contacts from the web interface too.

b. Wi-Fi and Bluetooth Networks

Information about saved Wi-Fi SSIDs and passwords is synced to Google's servers, as are any paired Bluetooth devices. Bluetooth information, however, is tied to your device ID, so Bluetooth devices paired to your phone won't sync with your tablet. Having your Wi-Fi networks backed up, though is a lifesaver - it prevents you from constantly asking your friends their Wi-Fi password when you're visiting them.

c. Phone Settings and App Installs

Google automatically backs up your phone's settings like the ringtone, vibration preferences, your home screen wallpaper and some app data. Certain app data (like your notification settings for Gmail) are also backed up this way. If you've added any custom words to your phone's dictionary, these will be backed up with your account as well. In addition, all data tied to Google Play such as the free and paid apps that you've installed are backed up with your phone. When you sign-in to your phone, it will automatically start downloading all the apps that were previously installed on your phones. Any in-app purchases that you had made will also be restored.

d. Google Account Data

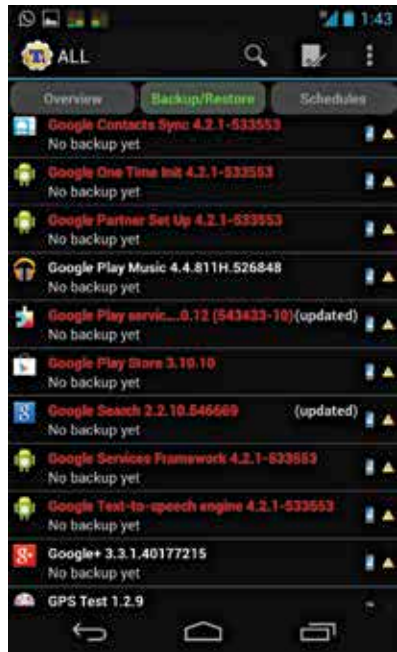
Lastly, data that is directly tied to your Google account such as Google Chrome bookmarks, Google Hangouts chat logs/chat groups, Gmail labels and filters, subscriptions to Google Play NewsStand and your reading progress in Google Play Books will be preserved across devices.

2. Titanium Backup (Requires Root)

The giant among all Android backup apps, Titanium Backup has been

around since the very early days of Android, and still enjoys a tremendous amount of popularity among Android power users, as the app requires your phone to be rooted. While the interface certainly feels a little dated, the sheer wealth of features the app provides are reason enough to give it a shot. The free version of the app can back up all of your user apps along with their data, and you can define schedules to automatically perform a backup of your user apps (or a subset of the apps, such as only the apps which have modified data) on a weekly basis. The real power of the app, however, is in the paid version, which unlocks the full set of features.

The paid version entitles you to multiple backups per app, backing up of system data, converting user apps to system apps (and vice versa) and deleting system apps (especially useful for removing bloatware). It also backups up your SMS/MMS/ Wi-Fi Passwords into an XML file for easy restoring. The batch backup feature lets you backup either all of your apps, only new apps or only apps with modified data in one click. Encryption is also supported - you can create a master key which is used to encrypt all your apps before backing them up, ensuring greater security. On versions of Android that support multiple user profiles (such as tablets running Android 4.2+), Titanium Backup will preserve profile information across backups. You can even restore data from Nandroid or ADB backups, irrespective of their format. If you've sideloaded an incompatible app, you can artificially 'attach' it to the market to ensure regular updates. If you're the kind who likes to flash ROMs frequently, Titanium Backup will create a single file called update.zip which contains all of your apps and data. While flashing the ROM in recovery mode, just flash this update.zip after the ROM,



Titanium Backup will backup your user apps, system apps and SMS/MMS messages.

and you'll have all of your apps restored when you boot up for the first time. The app will even modify system-level parameters like your Device ID if you want to move between different devices, clean up the Dalvik Cache or integrate system app updates directly into the ROM. Lastly, Titanium Backup will automatically upload your backups to either Dropbox, Google Drive or Box, ensuring redundancy of the backups. For the price of the app (~Rs. 250) you get a complete, end-to-end backup and restore, system, with full control over system apps, unlimited backup schedules and cloud backups.

3. Photo Sync (Dropbox / Google+ Photos)

The best camera is the one that's always with you, and for most of us, it refers to our smartphone. We all have photo libraries that are very dear to us, and thankfully backing up your photo collection is a piece of cake. Both Dropbox and Google+ support automatic photo backup to your respective cloud accounts, and you can configure it so that it backs up your photos (and videos) only when connected to a Wi-Fi network or only when your device is charging.



Dropbox will automatically upload all photos/videos when connected to a Wi-Fi network.

The Dropbox app for Android has this option turned on by default (accessible inside the Settings menu of the app), and will backup all photos that are stored inside your Camera folder. Google+ Auto Backup goes a step further, and can be used to automatically backup any folder containing photos on

your phone. To enable this option for other folders, open the Photos app, click on the Photos icon the top left > On Device > click on the cloud icon next to each folder name to enable/disable Auto Backup for that folder. Another advantage of using Google+ Auto Backup, is that any photo smaller than 2048x2048 pixels doesn't count towards your Google Drive storage, so you can store an unlimited number of such photos. Photos larger than this will show up in Google Drive and will count towards your storage limit. Additionally, you can use it to backup any PhotoSpheres that you may have taken, as they can be viewed properly only on the Google+ web interface. All photos uploaded to your Google+ account are private and are visible only

to you, until you change the privacy settings or choose to share them.

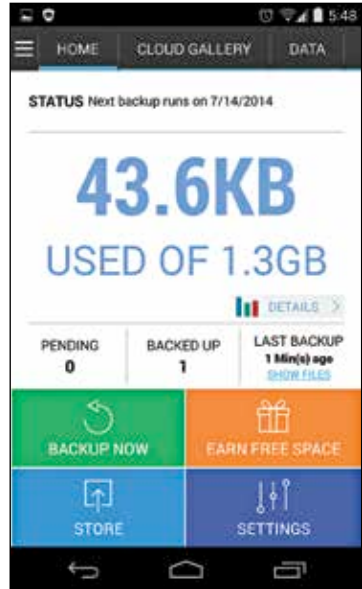
4. G Cloud Backup

If you're looking for an all-in-one backup app for your data, that's free and doesn't require root access, G Cloud Backup should be your app of choice. G Cloud Backup will collect all of your contacts, SMSs, music files, photos, videos, System Settings, browser bookmarks and calendar appointments and back them up to G Cloud's server. The data is transmitted over an SSL secured connection to prevent snooping. You get 1GB of cloud storage for free which can be increased through referrals or by sharing the app on Facebook/Twitter to upto 10GB.

Additional storage can be purchased directly through the app using in-app-purchasing.

Here's a step by step guide to using G Cloud backup to backup your Android device:

1. Download and Install the app from <http://dgit.in/GCloudBackups>
2. If you're using the app for the first time, sign up for a free account. If you've already signed up, sign in with your credentials.
3. On the next screen, you'll need to select all the different kinds of data that you want to backup. This includes your contacts, call logs, messages, photos, music etc. Bear in mind that the more you choose to backup, the more space you'll need.
4. Once you've performed your first backup, the app will create a schedule on which to automatically backup the selected items. If you wish to change the time/frequency of this schedule, head over to the settings. You can also disable the automatic backup if your battery is below a certain level.
5. Restoring data from your backups is as simple as heading over to the 'Restore' tab and selecting the items you'd like restored. This requires



G Cloud backup is a good app

an active network connection as the data has to be pulled from G Cloud's servers.

6. If the 1GB space seems too restrictive, G Cloud gives you several options for increasing your space without having to pay. The 'Earn more space' has a bunch of really simple tasks you can perform to earn up to 10GB of space.

5. Nandroid Backup (Required Unlocked Bootloader)

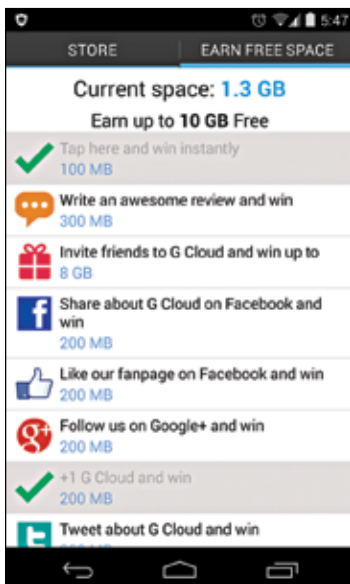
A Nandroid backup is a full-system backup image of your Android device. It contains images of each partition on your phone, including the /boot (the kernel), /system (the operating system), /data (user data and applications) and /cache. This

enables you to backup your entire system ROM, preserving the complete state of your phone at the time of backup. If something goes wrong while tinkering with your phone (a misbehaving app, a faulty setting or a bad kernel), you can simply restore the Nandroid backup, bringing your phone back to a previous state. Nandroid backups are a powerful tool, and require your device's bootloader to be unlocked. Most phones come with locked bootloaders, and with good reason. An unlocked bootloader can pose a security risk, as it allows anyone to modify the contents of any partition on the phone. Unlocking your bootloader will, in most cases, void your device's warranty.

The following steps detail how to make a Nandroid backup of your device, assuming your device has an unlocked bootloader. (The actual unlocking process varies greatly from device to device, so you should look up instructions specific to your device before proceeding).

a. Install a custom Recovery Image

A custom Recovery is a program that is installed on the /recovery partition,



The referral programme can help you earn more space

allowing you an alternate mechanism to interact with the phone, without touching the actual OS. The two most popular recoveries are Clockworkmod (<http://dgit.in/fitClockworkMod>) and TWRP (<http://dgit.in/fitTWRP>). For the purpose of this guide, we'll be using TWRP, but both recoveries are equivalent. Do note though, that backups are not compatible across recoveries, so a backup made in TWRP cannot be restored using Clockworkmod and vice-versa. Download the .img file, boot into your phone's bootloader using the ADB command :

- `adb reboot bootloader`

Once you're in the bootloader (again, your bootloader needs to be unlocked or this will not work), run the ADB command

- `fastboot flash recovery <name of the recovery image file>.img`

b. Backup Your System

You can boot directly into the recovery by running the ADB command

- `adb reboot recovery`

Once you're in the recovery, choose the Backup option, give a name for you backup and choose the partitions you'd like backed up. If this is your first backup, we suggest you check all of them. A full system backup will take up between 2-3 GB of space on your phone's internal memory.

c. Restore from an earlier backup

Restoring from an earlier backup is similar to the backup itself - boot into the recovery, and choose the 'Restore' option from the main menu. While restoring, you can choose among the list of backups on your system, and for each backup you can choose the partitions you want to restore.

6. Backup Using ADB (No Root Required)

Nandroid backups are comprehensive, but they need an unlocked bootloader, which can void your warranty. If you'd rather not go down that road, the ADB tool can backup up your entire system through the USB Debugging feature. This requires that you have the Android SDK installed, including

the tools like ADB and Fastboot. Installation links for different platforms can be found here - <http://dgit.in/SDKAndroid>.

We know that using the Command Line can be error-prone (if you type the incorrect command, or don't give the correct flags), so there's a handy GUI tool for Windows and Linux desktops that will do the job for you. Holo Backup (<http://dgit.in/HoloBackup>) works by connecting to your phone via ADB (you'll either need to connect via a USB cable, or if your phone supports wireless ADB, you can backup over Wi-Fi too). First, enable USB debugging on your device from Settings > Development > USB Debugging. Next, you will be prompted to authorize your PC to interact with your phone by confirming your PC's RSA fingerprint on your phone.

Then, simply open up the Holo Backup application on your PC, and choose the type of backup you want to perform. You can backup either your complete system, only your apps, the contents of your SD card (which includes your personal files like music, videos and photos) or a combination of these. You can backup your SMS messages to an XML file as well. Choose the destination folder to store the backups, and the tool will do the job for you. Restoring from a backup is also possible from within the same tool.

II. iOS

Apple's best-selling iPhones and iPads run iOS, an operating system that's always been more restrictive than Google's Android offering. This means a ROM-level backup like Nandroid is largely out of the picture. However, Apple's own offerings – iCloud and iTunes-powered backups, are well-integrated, seamless and fairly thorough, so there's no real need to consider third-party offerings.

iOS users can either choose to use Apple's cloud-based backup service, iCloud – which automatically backs up your data when your device is plugged in, locked and connected to Wi-Fi, or you can use iTunes backups, where iTunes backs up your data every time you connect your phone to your Mac/Windows PC. Of course, the two aren't mutually exclusive, and there's no harm in having both options handy.

Both iCloud and iTunes-based backups cover your data, including

- ▶ Photos, including your Camera Roll
- ▶ Contacts and contact Groups
- ▶ Call History
- ▶ Safari bookmarks, open tabs, web history and cookies
- ▶ Calendar Appointments

- ▶ Messages (both SMS and iMessage)
- ▶ Notes and Reminders (from the official Notes/Reminders app)
- ▶ Network Settings such as Wi-Fi / Bluetooth networks and devices
- ▶ Accounts (such as Email, Facebook and Twitter) and saved passwords
- ▶ Home Screen layouts and wallpapers
- ▶ Purchased apps, in-app purchases, application preferences and cache.
- ▶ Keyboard preferences, including custom dictionaries and language settings

Data that is synced to your iDevice such as music, videos and eBooks (either purchased on the iTunes Store or synced via iTunes on the desktop) is NOT automatically backed up by iTunes, but that shouldn't be a worry. If you purchased the media from the iTunes Store, your purchases will carry across devices, or if you've transferred media from your PC to your iDevice, it means you already have a copy of this data on your PC. Since iOS doesn't allow transferring music or videos through Bluetooth or even through Safari, you're unlikely to have any media on your iOS device that isn't already on your PC.

a. Using iCloud:

- ▶ Turn on iCloud backups by going to Settings > iCloud > Storage and Backup. Turn on iCloud if it's not already turned on.
- ▶ If you want to perform an immediate backup, click on the 'Back Up Now' option. This will initiate a complete backup of your iOS device to iCloud.
- ▶ To restore from an iCloud backup, you need to use the iOS Setup Assistant, which is run only while setting up a new device (or if you've wiped your device and restored it to factory settings). If you're setting up a new iOS device, choose the 'Restore from iCloud Backup' option,



Just slide it on

and select which iCloud backup you want to restore data from. If you wish to restore data from an iCloud backup on a device you're currently using, you'll first have to wipe all data from the device. Tap Settings > General > Reset > Erase All Content and Settings to wipe your device, and follow the steps in the iOS Setup Assistant, choosing the iCloud restore option.

b. Using iTunes

Using iTunes could be a good idea if you have a slow or unreliable Wi-Fi connection, or if you have a lot of data to be backed up (iCloud only allows you up to 5GB of data for free). To use iTunes to backup your iOS device,

- ▶ Turn off iCloud sync from the Settings > iCloud > Storage and Backup menu.
- ▶ Connect your device to your computer, either using a USB cable or wirelessly, from Settings > General > iTunes > Wi-Fi Sync.
- ▶ Once iTunes detects your iOS device, go to the devices page (either from the button on the top-right or from the left sidebar). Here you'll see detailed information about your device, along with a button that says "Backup Now". You can also choose to encrypt your backups using a password. You'll need to provide the same password while restoring from this backup.



Backup using iTunes

- ▶ iTunes backups are stored in the following locations, depending on the Operating System your PC is running:
 - Mac: ~/Library/Application Support/MobileSync/Backup/
 - Windows XP: \Documents and Settings\username\Application Data\Apple Computer\MobileSync\Backup\
 - Windows Vista / 7 / 8 : \Users\username\AppData\Roaming\Apple Computer\MobileSync\Backup\
- ▶ To verify that the backup has been created, you can open the Preferences window in iTunes and go to the Devices tab. You'll find a list of all iOS device backups present on that computer.

If you've set your iOS device to automatically sync with iTunes whenever it's plugged in, it will automatically perform a backup every time you connect your device to your computer.

III. BlackBerry

Similar to iOS, Blackberry also allows you to backup your phone's data to either Blackberry's servers or to your own desktop. To backup to Blackberry's

servers, you'll need to install the BlackBerry Protect app, a free app available on the BlackBerry AppWorld. Backing up your BlackBerry phone to your computer requires the BlackBerry Desktop software or BlackBerry Link, depending on your OS version.

1. Using BlackBerry Desktop:

- ▶ Download and install the BlackBerry Desktop program to your Windows/Mac PC from <http://dgit.in/ftBBDesktop> (for older devices running BlackBerry 7.1 OS and earlier) or the BlackBerry Link software from <http://dgit.in/ftBBLink> for smartphones running BlackBerry 10 or newer.
- ▶ Plug in your device using the USB cable and select Backup Now. You can choose between backing up your entire system via a full backup, a full backup sans email messages or a custom backup containing only a subset of your data. If this is your first backup, we recommend a full backup.
- ▶ To backup files contained on your Internal Storage (such as photos, videos and music), check the box next to 'Files saved on my built-in media storage'.
- ▶ You can encrypt your backups using a password for added security, select the checkbox next to 'Encrypt backup file'.
- ▶ Restoring from a back up is pretty straightforward, use the 'Restore' option and locate the backup file you had created earlier.

2. Blackberry Protect

If you want an automated backup system that doesn't need you to tether your phone to a computer, BlackBerry Protect is a free app that backs up the contents of your phone to BlackBerry's servers.

- ▶ Install the free app from BlackBerry AppWorld
- ▶ Sign in using the your BlackBerry ID and select the data you want synced.
- ▶ Choose a backup interval.
- ▶ You can choose to enable Location Reporting, which will help you find your device in case you ever misplace it.

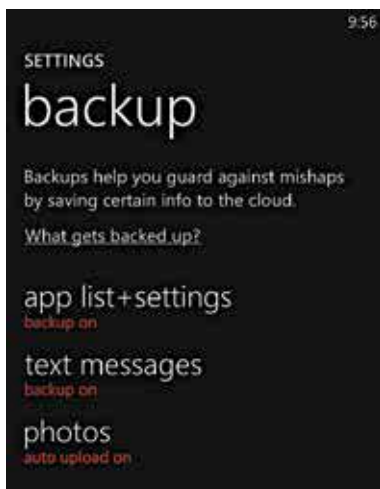


BlackBerry Protect is an automatic, over-the-air backup app for your phone.

IV. Windows Phone

Devices running Windows Phone 8.1 have a built-in backup service similar to Apple's iCloud. This can be found inside the Settings App. Navigate to the Settings > Backup.

- ▶ Inside the Apps + Settings menu, turn on the Settings Backup option via the toggle switch. Once the Settings Backup is switched on, turn on the Apps Backup as well. What this does is backs up your system data, including the apps you have on your phone, any in-app-purchasing, your progress and high-scores in games, your call history, Internet Explorer bookmarks, Start Screen layout and theme colour, saved passwords and any social networking accounts you may have set up on your phone. General phone settings such as your lock screen settings, custom dictionaries or push notifications settings will be backed up as well.
- ▶ Next, you can backup your text messages by turning on the “Text Messages” setting from within the Backup menu. Note that simply turning off this setting will not automatically erase all your texts.
- ▶ The Photos + Videos setting will backup all the Photos and Videos stored on your phone to the cloud, in a quality of your choosing. You can choose between the bandwidth-efficient “Good Quality” setting or the “Best Quality” setting. Photos and Videos are uploaded to OneDrive only when your phone is connected to a Wi-Fi network.
- ▶ Restoring data is a little simplistic, and you can only restore from your backups when you're setting up a phone for the first time (or after a factory reset). While setting up, log in using your Microsoft / Outlook / Live account and your backed up data will automatically finds its way back to your phone. 



Windows Phone's built-in utility will backup your texts, photos and settings.

SAVE UP YOUR PASSWORDS

Yes even passwords can be backed up.
Go through this chapter and you'll never
lose another password ever again. In fact
you won't have to remember one in the
first place.

This story begins with man and his little internet companion, Passie. They were inseparable as little Passie helped our hero explore the wide world of interconnected computers. Passie became a part of our protagonist's browser until certain security issue forced our central character to replace 'ol Passie with a new combination of keys.

It is at this juncture that things take a turn for the worse. The original Passie was tried and tested. And more accounts were opened online, she became the key that unlocked each door. But the new Passie was born out of a last minute thought and impatience because a whole



If only it were that easy!

bunch of websites going the open source way when it came to security. The new Passie was also pretty inconsistent and logging in was never the same again.

This story teaches us one very valuable lesson and prompts us to give you one solid piece of advice. The former is that remembering the passwords to all your accounts is nigh impossible and using the same password for every account is a pretty stupid idea. Even if you are an eighty year old grandmother of seven and just getting the hand of the world wide web. In the event some malicious hacker gets a hold of your password and other credentials from one website, his or her (yes, girls can be hackers too) first reaction would be to try it out at all the possible places you might frequent and gain access.

So it is at this point that we feel we should introduce you to the magical world of (say it with us now,) Password Managers.

Huh?

If you involuntarily grunted that that syllable, a password manager is an application that organises the different passwords you use. Each account has its own entry and some will auto-fill forms with credentials you have entered previously. They are also smart enough to tell if the website you're on is the real deal or not too. These passwords can be stored locally or on the cloud. Quite a few come as browser plug-ins and equal number, if not more as smartphone apps. Some even manage PIN numbers for you and all of these passwords are kept perfectly safe by a very strong master password.

“A very strong master password that anybody can guess/ get out of you and steal all the money in your bank account(s),” said most of the people that read the last line of the previous paragraph. But here is where the devs have outsmarted us once again. While all (we hope) password managers require a master password for access, a few can be plugged in to fingerprint scanners and a few even use Google's Authenticator, which generates one time codes and sends it to your mobile. There's an app for that too by the way.

Can ya tell me more son?

To talk in detail about all the different password managers out there is a difficult task. One can recite names off a list ad nauseum and the list will still keep going and you'd be left with a messy floor. Instead, allow us to introduce you to a few that truly outshine the software that jumped on board the 'me too' wagon or are sold as part of bundles.

LastPass

Despite being a pretty ironic way to start this list, LastPass happens to be one of the best managers in the market and that's not even the best part. The best part is that it's free.

Available at lastpass.com, LastPass is available on Windows, Mac, Linux on the PC platform and on iOS, Android, BlackBerry, Firefox Mobile and Windows Phone. It's also compatible with portable versions of Chrome and Firefox web browsers where it can be installed on to a USB drive and used by people who end up using public computers for their day to day activities.

The only downside is that if you want to access the mobile versions, you need to go pro. Then again, that's your only reason to go pro. Pretty much everything else is there in the free version.

Once you've downloaded and installed LastPass on your computer,



Saving you trouble in over 113 countries.

you are sent through a whole bunch of steps where early on you decide whether you want to install plug-ins for your browsers. Once the installation is complete, you are required to create a LastPass account and protect it with a master password. Like most places you can type in a phrase or a clue that will help remind you what the password is in case you forget. LastPass also offers to search your computer for all the user ids and passwords that it can save, but you can choose not to do that either.

Now that the basics are out of the way, let's get down to figuring out how it works. What you installed on your computer is your LastPass Vault. All your passwords are saved here. But before you actually get down to using it properly, you need to set it up. The best part is that LastPass grows with you as you log in to different accounts. As soon as you log in, the browser plug in (if you've installed it) asks you if you want to save the credentials to that particular account. In a few cases like net banking you might need to set it up beforehand, but for your mail and social media accounts, it works straight out of the box.

With LastPass you can save any sort of sensitive information including credit/debit card credentials. The autofill feature which works rather well

can be used to streamline your shopping experience too. Tired of wasting precious seconds keying in your valuable information? Well, waste no more with LastPass.

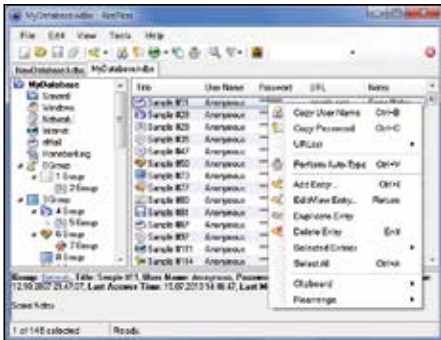
KeePass

Staying in sync on the nomenclature front is the next product on our list. KeePass is a free, open source password manager that works on Windows, Mac, Linux and Mobile. The fact that it can boot off a USB drive makes things a lot more interesting. But you're not going to get any self learning, auto form filling magic. Just a master password and a database of every account you keyed in.

Once you've installed KeePass, you are greeted by a pretty basic interface. Clicking on the 'New' button lets you start a new database with its own separate password. Once your database is named, you can get down to business. The entire interface is divided in two. The left side contains a list of nested directories and the right displays the contents of each. Right-click on the right and you can create a new entry. Once done, you can individually copy usernames and passwords or you can make it do tricks by hitting Ctrl + V. This is the auto-type command and KeePass automatically switches between itself and the appropriate dialogue boxes and

fills it up. Just make sure the correct website is open in the background and not MS Word.

The really cool thing about KeePass is that it supports plugins. There are a lot of them out there which slowly, but steadily take KeePass up to the level of anything else in the market. Plugins like KeeFox and ChromeIPass allow you to



Getting this does not make you something that rhymes.

link your KeePass database to your web browser enabling auto-filling, password management and more.

If you save your database to your dropbox folder, you can connect the appropriate apps for other devices to the database and sync your accounts across all your devices.

Everything you could possibly need is available at www.keeppass.info. You can even pick up versions of KeePass developed by others along with the mobile versions in the download section. Sadly they're both filed together.

Dashlane

Dashlane is yet another password manager and this one too is available for Windows, Mac, iOS and Android. The only difference is that the mobile applications are legit and free. It's got a very clean interface and prides itself in the fact that you will never need to fill a form or physically log in to an account ever again. As soon as you've installed it, you're prompted to install the appropriate browser extension and you're good to go.

By entering your name, date of birth, title and phone number, Dashlane claims to auto fill every account for you and the browser extension automatically imports all your credentials. On startup you are also presented all the accounts/websites you frequent/ have saved credentials on your browser for. All you need to do is click a and presto! If you prefer to use your browser's address bar and a web address to get you to your destination, the accounts against which entries exist have a tiny blue gazelle inside the fields. Clicking on any one autofills the entire thing. But it somehow managed to import incorrect information into one of our accounts so you may want to watch out for that.

The digital wallet service provided is pretty nifty too. This coupled with auto fill makes online shopping a breeze because your address is filled in for



Keep track of everything.

you. The really cool thing is that Dashlane claims to curate all your receipts and helps you keep track of all your orders.

All the above features are available on the mobile apps too. Even the digital wallet. But if you want to make life easy and sync all your devices or take a peek at your passwords from a remote location, you're going to have to go pro and fork over \$ 29.99 every year. But then again, nobody got rich by being impatient or lazy.



It's available everywhere!

Roboform

Last on our list is Roboform and Roboform likes to learn. As you log in to each account, Roboform saves the login details and logs you in automatically the next time.

Once the installation, the master password and the mnemonic that you thought up to remember your password have all been taken care of, all you need to do is open Roboform and start browsing. As you log in to your accounts, Roboform offers to remember your credentials for you.

These accounts can be accessed from a dropdown menu aptly titled 'Logins' and life is beautiful once again. Well only for ten accounts on the free version. Everything else is the same.

Signing up is pretty standard. Just give it what it asks for and we're all set. For some reason, the passwords that are considered moderate by the other managers mentioned here are considered excellent.

A very interesting feature Roboform provides is Roboform Everywhere. It's a bookmarklet or a bookmark which can run a tiny Java Application. Once you've logged in to your Roboform account online, all you need to do is hit the tab that says 'Bookmarklet'. The page this will take you to where you can find the bookmark. Just drag and drop the link to your bookmarks bar and you're set.

If you click on the bookmark from anywhere in the world, you can access all your saved information ranging from passwords and log-ins to notes and pin numbers. It doesn't exactly work on your mobile's browser, but you still can log in to your Roboform account and look up passwords

But, why do that when there's an app for that? The Roboform mobile apps are free and you don't have to worry about manually entering your details each time you want to access it because it syncs across all devices! Hallelujah! But, like the free version of the software itself, you will need to buy a license is when you've exceeded the 10 login limit. Find everything you need at www.roboform.com.

While these are just four of the many password managers out there, it's important to note that a lot of the ones out there possess a few similar features.

For instance, they'd be able to generate complex secure passwords at the click of a button and save you the trouble of remembering them.

They'd all give you military grade encryption for your account and its data.

You can unzip a specialised version on to a flash drive and run the program off it. Make things even more secure by booting it off a thumb drive with a hardware encryption. The same USB drive could also act as a password to log in to your account too.

If you're an international spy and you're worried about key-loggers, then you can use the onscreen keyboard that most software offer.

While password managers may seem like they've come from to save you and take you to a better places, there are risks involved and the biggest one is probably reading this. Your accounts are as safe as your master password is strong. If it can be guessed, then



Looks can be deceptive

god be with you. The second biggest risk is directly related to the first because all your saved passwords are in one place giving your nemesis access to everything from your wife's birthday to your credit card.

But there are a few things you can do to keep these details safe. For starters, don't leave your computer open and logged in. Then maybe you could not share these details with others. Try using something like a biometric scanner as a means of access and please don't share the details of your account with anyone. Also get a good master password and lock your computer or device with a password when you're not using it. 

BACKING UP MISCELLANEOUS DATA

In our quest to back up our digital life, we often forget the little things – bookmarks, saved games, sticky notes, contacts, form data and registry entries. This chapter will show you how to never leave anything behind.

Life in the digital world is incomplete without the web. And when you're talking about the web, you're talking chaos. Just as we'd tackle any clutter, we need to form a strategy before going about finding the right backup solutions. When it comes to the web, there's no set strategy. This is because unlike operating systems, which are complex and enforce certain rules upon the user, the web browser is relatively very simple and each user can interact with the browser in different ways.

Sync your web browser

The kind of synchronising required for web browser data will differ from person to person. Take for example a contrast of two very different person-

alities. One kind hardly searches for stuff and gets his recommendations from social media. This is someone who doesn't save too many bookmarks and enjoys reading material that he deems interesting on his Twitter or Facebook feed. He might not bookmark pages he goes through and isn't bothered whether he's logged in to Google when utilising its search engine. Such a person has hardly any browser data to back up.

The other kind searches for precisely what he wants to read, and is subscribed to blogs and new feeds. He has a long reading list, is up to date with latest developments in his field of work and probably has a list of videos and pages to go through. Such a person would need many tools to back up his digital life.

Most web browsers today come with a sync service built in. Mozilla Firefox, Google Chrome (and Chromium browser), Internet Explorer, Opera and Safari each have their own sync servers. All you need to do is log in to the service/s via one of these browsers and all your tabs, history and bookmarks are synced and immediately available on your other devices. Syncing your web history and bookmarks are no longer a problem as long as you're using the same browser across your devices (which can be an issue if you're addicted to either Internet Explorer or Safari, since both have limited presence across multiple devices).

Sync your contacts

If by any chance you happen to be a Mac and/or iPhone user, you won't have to worry about syncing your contacts. Once you associate your Apple ID with all your devices, they all get the same contact list as and when Apple contacts its servers over the internet.

For the rest of humanity, the non-Apple owners, you probably need to take a few steps to ensure your contacts are always up to date. Google is the best possible solution for this among many others, including Microsoft.



Apple allows you to sync with many services

The CardDAV protocol

Truth be told, you can sync and store contacts in so many ways that it isn't possible to individually fit them into the pages we have left. So let's delve into just one of the strategies here. Regardless of whether you own an Apple or non-Apple device, the contacts syncing is done over a protocol known as 'CardDAV' (<http://en.wikipedia.org/wiki/CardDAV>), which is supported by many clients. To sync contacts, you need a server which stores the contacts and supports the CardDAV protocol and a client which can understand the



CardDAV at work

CardDAV protocol. This ensures that the contacts are obtained from the server and any updates to those contacts are pushed as well. If a service provider is as famous as Google, the clients would have the URLs figured out and all you need is a username and password.

There's a good chance that you (or your organisation) use Google's services to sync contacts. In that case, most email clients and smartphones will simply let you enter your Google credentials to sync your contacts. However, if you don't have a Google account, the first requirement to sync your contacts is the ability to publish your contacts list over

the CardDAV protocol. Unfortunately, this won't be possible if your contacts service provider is unwilling to support the protocol. For example, Microsoft with its Outlook.com platforms seems to be unwilling to let anyone access its contacts and calendar services.

Most smartphones are capable of adding most popular calendar services such as that of Apple, Google and Outlook.com. In case your phone doesn't support it right away, you can try adding a 'CardDAV' account. If the OS doesn't support it on its own, you can download and install apps, which enable the functionality (for Android, go to: <http://dgit.in/PlayStoreCardDAV>). Once done, enter the URL for your calendar, and the username and password on the server (which should be your username and password with the service provider) and you're all set. For example, if you have an OwnCloud service running on your own server where you'd like to sync your contacts, you can log in to OwnCloud's web interface. Click on the contacts app on

the left, then on the gear icon (settings), followed by the little globe icon. This should bring up the URL, which you can feed into a CardDAV client to access and sync your contacts to the server. This URL is what you can use to access your contacts.

Add-ons and extensions

Apart from this, multiple tools and add-ons can be used along with desktop clients such as Thunderbird to make syncing your contacts easy as pie. A notable extension to Thunderbird in this area is 'gContactSync', which you can either search for in the Add-ons manager built into Thunderbird or download from: <http://dgit.in/gContactSync>. Though Outlook doesn't allow contacts to be synced with Google, a tool named 'Contacts Sync' (<http://dgit.in/ContactsSync>) promises to bring in the ability to do so. If you use Google Apps for Business with Outlook, a tool has been made available by Google itself, which you can download from: <http://dgit.in/GAppsSync>.



gContactsSync at work

That was about syncing contacts. If you want to back them up, almost all clients and service providers will give you an option to download the contacts in a format compatible to your system (in most cases, you get a VCF format file which can be shared with others as well).

Sync your calendars

Being popular has its advantages. Say, if you're trying to sync calendar services belonging to Google, Yahoo, Apple or Microsoft Exchange service over multiple devices, it's quite easy to do since most devices support them.

Just as the CardDAV protocol is used to share contacts info, the CalDAV protocol is used to share calendars. Here, however, we have a mix of different standards and different ways to achieve this. If you simply want to

back up your calendar, in most cases, you can do so only in the ICS format used by Apple's iCalendar program.

Sync Google and Outlook Calendars

If you want to add a calendar to your smartphone, it must support the CalDAV protocol; and if it does, you'd need three things – your calendar's URL, the username and the password. This, however, isn't always possible. For example, we couldn't find a way to share our Outlook.com Calendar over CalDAV. The only options it would give us was to download the calendar in ICS format, to view it on the web or to subscribe to it via feed (which is understood by other calendar programs). Similarly, Google also wouldn't allow CalDAV access to the calendar right away. It would be rare for your calendar client to not provide an easy method to sync with Google Calendar. However, if you happen to find yourself in this rare situation, there's still a way to do it – by creating a Google App. Don't worry, no programming required here. You'll just be creating an app in the console provided by Google). Go through the guide at: <http://dgit.in/GCalendarAPI> and you should be fine.

Sync iCloud Calendar using CalDAV

To use CalDAV with Apple's iCloud Calendar is a little tricky:

1. Start the Calendar program in OS X.
2. Click on the 'Calendars' button on top. This opens up the left sidebar with the calendar list.
3. Hover over the calendar name and you'll see the sharing icon (this looks like a Wi-Fi icon). Click the icon. Now click on the checkbox named 'Public Calendar'. A link will be created that looks like this: `webcal://p17-calendarws.icloud.com/ca/subscribe/...`
4. Notice the number after 'webcal://p'. In this case, it's 17.
5. The CalDAV URL that you need to use is: <https://p17-caldav.icloud.com>. Remember the 'https' in the beginning.
6. The username for this is your iCloud email address. Remember that it's not your Apple ID. So if your Apple ID is digit@gmail.com and your iCloud email address is digitindia@icloud.com then you should use digitindia@icloud.com as your username/email address. Remember to provide the password for your Apple ID.

On Android, it's possible that you wouldn't have native CalDAV support. In that case, you can download the 'CalDAV Sync Free Beta' program

from <http://dgit.in/CalDavSync>. Once the app is installed, go to settings menu where you'd have a new entry that will allow you to add CalDAV accounts. Use it to sync with your iCloud Calendar.

If you have an OwnCloud installation, you can use the same too. Just log in to your OwnCloud installation and open the calendar app on the left. Then click on the Settings gear icon on the top right. You should get the CalDAV address for your client.



Apple allows you to add different accounts

Back up your Windows Registry

To 'sync' the Windows Registry makes no sense because of the way it's built. The next feasible thing is backing it up. But why would someone want to back up the registry? Registry is the central configuration storehouse of Windows. The OS itself stores its settings and allows many other apps to store their settings in the registry. So, if someday you find yourself supremely satisfied with the way you've set up all your software and OS, you might want to back up the registry. So in case something goes wrong with settings, you can simply restore the backup and be at peace again.

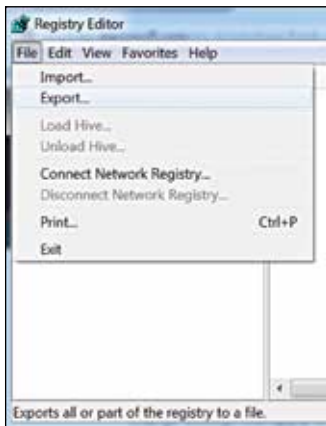
The process of backing up the registry is pretty straightforward:

1. Launch the registry editor by opening 'regedit.exe' (use the Start search)
2. Allow access via UAC prompt
3. Select the 'Computer' entry at top
4. Go to File > Export
5. Save the backup file in any location you want.

Opening the file automatically restores it. Remember, however, that if you want to restore your settings across Windows installations, this backup may not work well, mostly because there are a lot of IDs stored in Registry (notably the User IDs), which are freshly generated every time you install Windows. This method leaves behind certain hives and the restoration may not always have the effect you wanted. If you want a more robust tool, you might want to try the Registry Backup tool from <http://dgit.in/RegistryBackup>.

Back up saved games

While some games might save user settings, player's progress and saved games in the Windows Registry, most save their settings in flat files confined to a single folder. In most cases, if you back up the saved game folder from a PC and restore it, your settings and game progress will be restored as well. The main challenge is finding out where the saved game folder exists. While searching for your favorite game's location would work well, if you have a number of games installed then you can use a tool to find them faster. Gamesave Manager (<http://www.gamesave-manager.com>) is a nice tool with an adequately large database of game-save locations for different games.



The registry editor

Sync your notes

From Box to Dropbox and beyond, there are enough cloud services to sync your important documents, but what about notes? Many, if not all of us, don't use a word processor for taking notes. Some of us use Windows' sticky notes widget to keep ourselves on track regarding important work. We end up storing phone numbers, URLs, passwords and what not on these widgets and sometimes it's just as important to back these up as well. In Windows 7 and above, your sticky notes are stored in a folder under your profile directory. To open the folder, go to run prompt and type "%AppData%\Microsoft\Sticky Notes". Inside that folder are all your sticky notes stored in a file called 'StickyNotes.snt'. And if you want your notes to continuously sync in the cloud, you have a beautiful and powerful client in Evernote. 

RECOVERY - FOR THOSE WHO DIDN'T BACKUP

This chapter tackles some of the questions regarding data recovery that may possibly be nagging you

Data recovery...So we've come to this now, eh? If only we had all just backed up our data like we were supposed to. If you're reading this chapter with a little more interest than usual, then you either already messed up with regards to your data, or aren't confident about your ability to stick by what we've already told you about backing up your data. Before we talk at length about data recovery, the way it works and whether or not it works at all, you should be warned that data recovery is the absolute last measure to fall back on – always rely on backups.

To answer a question that must be on many of your minds – Can we recover data from damaged hard disks, or data that we've (apparently) permanently deleted? Luckily, the answer is yes. However, the process isn't entirely smooth or efficient. In some cases, depending on the extent



Are deleted files still on your hard disk?

of damage, it can be very expensive as well. Whether your data has been accidentally deleted, your drive been formatted, your entire data swept away by a virus or even the drive no longer being recognised by the operating system – you still don't need to enter into panic mode com-

pletely. Many times, the data is recoverable, and fortunately, there's a bunch of file recovery programs to help you do this on the cheap, if not for free.

How does recovery software work?

So, how does this kind of software work exactly? When you deleted your data from the recycle bin, the command prompt did say that you were deleting it “permanently”. Then how are we able to magically resurrect this piece of information from its grave? Well, the truth is, deleting data is a bit more complicated than simply erasing a piece of information from the drive. Surprisingly, in fact, the data isn't actually removed from the drive when deleted. The files are just not accessible in the way they were anymore. For example, if you delete a file, the file's data isn't erased from the drive, but a signature byte is placed at the location of the file informing the OS that the area can be overwritten by other data next. In other words, the file system marks the areas that previously contained the file as free space that can now be overwritten with new data if need be. The file is now invisible to the operating system and as a result, to you. It's precisely this hidden state of which the file recovery system takes advantage – it knows that though the directions to the file are missing, the file essentially isn't. And this isn't just the case with your computer hard disk. Files are deleted and stored in a similar manner when it comes to your SSDs, external hard drives, iPods, CDs, USBs, etc. So yes, deleted data can be recovered from any of these data storage devices – although, the particular program must support the storage device in question. Recovery works even in what seems like the most extreme of cases – when you've formatted a drive from FAT32 to NTFS, and suddenly realise that you didn't need to do it since all your files were still there. Luckily, when you format a FAT32 drive, everything is destroyed but the partition table and the data – and that's all we need! Since the data's still there, your files can still be reconstructed.

How long after the error can I still recover my data?

That isn't exactly the right question, to be honest. For recovering data doesn't depend on the time, but on how much data you've written to the drive since deleting it. We just talked about how the data is still available on the hard disk, but is just invisible to the operating system. So basically, whenever there's data to be stored on that drive, the OS might just allocate the now free space to it, thus overwriting the data that was already present there. If this happens, then you can be absolutely sure that there's no chance of recovering that data.

Hypothetically, if you delete a particular file, immediately shut down your computer and don't operate it for another ten years, you should still be able to recover that file once you start the computer again (provided it's still in working condition, and your mom/spouse/roommate let you continue to keep that thing in the house). If, on the other hand, you continue to use your computer normally, store some videos, browse the internet etc. there's a very high chance that the file recovery process may not go as well as you'd hoped, as the existing data might have been overwritten by the new data.

So you need to be extremely careful about the next step once you've realised that your data is gone if you want to recover that content. Sure, there's the slight chance that the OS might place new data in some section of the disk that isn't occupied by the old data – but there's great risk associated with that. Even if you download, let's say, 1 MB of new data, there's the likelihood of it being stored in an area, which belonged to a 100MB cluster – thus possibly corrupting the entire 100MB file. That's one of the reasons why even surfing the internet immediately after the error (possibly to look for recovery tools) is discouraged, because the browser automatically begins to download files on to your hard disk without your permission (even if you've disabled cookies). This might just overwrite some of your existing data. That's one of the reasons why if there's an option to choose between portable recovery software and installed software, try to go with the portable option.

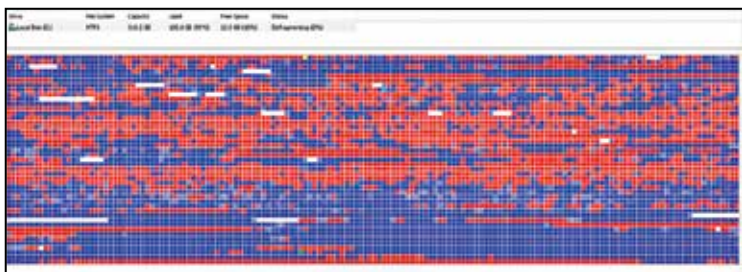
Considering that the best way to recover data requires that you not even run the drive anymore, it's better to take into account other feasible options – such as getting an additional drive. Since this drive is not in peril of losing its data, load the recovery software onto it. Only then, will you attach it to your computer and its “bad” drive and run the software to recover as much data as possible from your PC's hard disk. Doing this

allows as many additional downloads as possible to happen on the extra drive without hindering the recovery process.

Right at the end of this chapter, we've given you a list of some free recovery software that we think should do the job for you. In the meanwhile, let's move on the next section of this chapter.

What is the efficiency of the recovery process?

Many times upon trying to recover some data, you may find that very few of the lost files will be 100 per cent recoverable. Why is that the case? Why are only parts of the data recoverable? Will it be usable? Well, the answers to these questions lie in a fact we've already mentioned previously. We spoke about how data is stored on your drive in clusters – but the thing is, these clusters aren't necessarily all stored next to each other and in one place. They're usually stored in different parts – this is called 'fragmentation'.



So many sectors so little time

Even the smallest of files could be heavily fragmented and spread over a hundred different parts of a hard drive.

If you've ever defragmented your disk, you'd already be familiar with the concept. In case you're not, Windows users could head over to Start > System and security > Administrative tools > Disk Defragmenter > Select drive > Defragment Disk to view its graphical representation.

So, when the computer sees a bit of space that could be overwritten, say, the space occupied by only 10 per cent of a particular file, with the remaining 90 per cent in parts elsewhere, it allows a new file to take up that space. This is what prevents recovery software from successfully retrieving some files in their entirety. A file's usability depends on the type of file it is and the parts of the file that are missing. However, recovering a file that's had its data overwritten on by a new file's data usually proves futile.

So essentially, in most scenarios that include logical failures such as accidental file deletions, formatting, power failures, virus attacks etc., you don't need to be a computer expert to be able to recover your data safely and inexpensively. Just make sure that you use recovery tools and not repair tools that might write to the disk. However, there are some cases when data recovery software just won't cut it, which brings us to the next question you may have...

When do I need to go to a professional?

There are cases where the drive stops functioning because of a physical problem with it – the drive isn't spinning or is making strange noises. When a hard drive is physically damaged, software solutions won't help you. You're then left with no other option except turning it in to a data recovery expert.

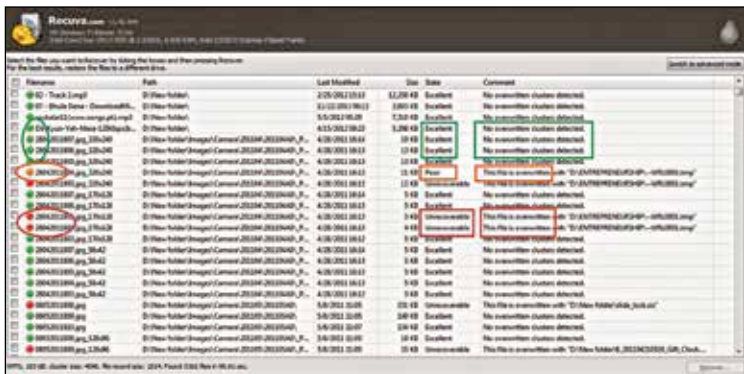
Worst case - you can get professionals to recover your data for you.jpg
Caption: Worst case - you can get professionals to recover your data for you

Be advised, however, that most of these recovery processes end up being an expensive affair with the price usually depending on the amount of data that must be recovered.

Free recovery software

Here's to hoping, though, that your data recovery problem can be solved at home using software. Listed below are some few free software that we think can possibly be the solution to your problems:

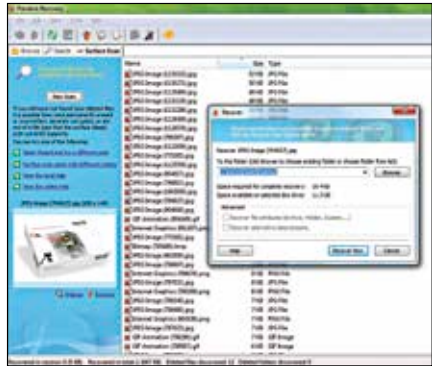
1. **Recuva (Windows):** Arguably, the best free file recovery software that's available. It can recover files from your hard disk, external hard disks,



Recuva shows how some files are unrecoverable

DVDs, CDs, memory cards and even your iPod! Recuva's file recovery wizard comes in handy for searching for specific types of files and looking for them in precise spots. Any files that are found are listed (with previews for images) and can immediately be restored with just a couple of clicks. It also has an advanced mode, which provides a much deeper scan as well as the option of wiping out files so that they can never be undeleted again. This is a useful feature for people recovering data only to ensure that particular files are truly dead and gone.

2. **Testdisk (Windows/Mac/Linux):** A powerful Open Source tool, this software is available across all platforms. It's an extremely powerful tool that not only lets you recover accidentally deleted data, but also helps rebuild your boot sector, fix FAT tables and find lost partitions to help locate data, among other things. The only downside to this tool is that it has no GUI, and hence isn't extremely intuitive.
3. **Pandora Recovery (Windows):** If, however, a really helpful wizard and an easy-to-use, interactive UI are your priorities, then Pandora Recovery is a suitable choice. It's extremely user friendly, and though the initial standard search may not seem to recover many files, the advanced 'Surface Scan' should do the trick and recover most files. The Explorer-like folder view and excellent search tool make recovering data with this software a breeze.



4. **PhotoRec (Windows/Mac/Linux):** This software is actually bundled along with Testdisk, but it deserves a separate mention, since it's a safer alternative for times when deep disk recovery or screening through your partitions isn't required. This is another extremely powerful tool that doesn't really have the best user interface, but it makes up for this shortcoming by its ability to work with most file systems and device types and, despite its name, isn't just relegated to photos.

There you have it. Hopefully, these software solutions are good enough for your problem. We wish you a quick recovery. 



All this and more in the
world of Technology

VISIT
NOW

▶ **digit.in**

Join 200K+ members of the digit community



<http://www.facebook.com/thinkdigit>

facebook

digit
thinkdigit.com

Digit 1,234 likes
Product

Your favourite magazine on your social network. Interact with thousands of fellow Digit readers.

- Wall
- Info
- Notes
- Event
- Photos
- Video
- Links
- Pages
- Groups
- Places
- Events
- More

<http://www.facebook.com/IThinkGadgets>

facebook

I Think Gadgets 1,234 likes
Community

An active community for those of you who love mobiles, laptops, cameras and other gadgets. Learn and share more on technology.

- Wall
- Info
- Notes
- Event
- Photos
- Video
- Links
- Pages
- Groups
- Places
- Events
- More

<http://www.facebook.com/GladtobeAProgrammer>

facebook

Glad to be a Programmer 1,234 likes
Community

If you enjoy writing code, this community is for you. Be a part and find your way through development.

- Wall
- Info
- Notes
- Event
- Photos
- Video
- Links
- Pages
- Groups
- Places
- Events
- More

<http://www.facebook.com/devworx.in>

facebook

devworx 1,234 likes
Community

devworx, a niche community for software developers in India, is supported by 9.9 Media, publishers of Digit

- Wall
- Info
- Notes
- Event
- Photos
- Video
- Links
- Pages
- Groups
- Places
- Events
- More